(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002149061 A**

(43) Date of publication of application: **22.05.02**

(51) Int. Cl **G09C 1/00**
G06F 12/00
G06F 12/14
G06F 15/00
G06F 17/60
G06K 17/00
G06K 19/00
G06K 19/10
H04L 9/32

(21) Application number: **2000348531**

(22) Date of filing: **15.11.00**

(71) Applicant: **NEC CORP**

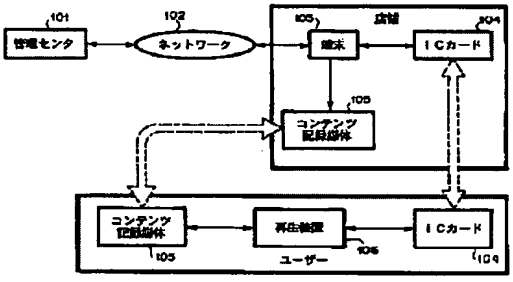
(72) Inventor: **OTA KANTARO**
SOEDA NAGAKI
TSUKAMOTO YUJI
KIKUCHI YOSHIHIDE
FUNAYA KOICHI
OTSUKA OSAMU

(54) **RENTAL CONTENTS DISTRIBUTION SYSTEM AND METHOD THEREFOR**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a distribution system and method for improving benefit and convenience of a user, eliminating the profit loss of a shop, and safely protecting contents in the distribution of the digital contents.

SOLUTION: A reproducing device 106 and an IC card authenticate each other; the IC card and a control center 101 authenticate each other; the IC card transmits a reproducing device public key certificate received from the reproducing device to the control center; a terminal receives contract information including a contents title and a rental period from the user; the control center receives the contract information with the signature by the IC card; the control center ciphers a contents ciphering key or the like by using the reproducing device public key or the like and sends it with the signature to the terminal; the terminal writes it in the IC card; if the result of the signature collation is correct, the terminal records the contents in a recording medium 105; the reproducing device 106 decodes the cryptographic key of the ciphered contents received from the IC card and decodes the contents by using the same.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－149061
（P2002－149061A）
(43)公開日　平成14年５月22日(2002.5.22)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ　５Ｂ０１７
			６４０Ｚ　５Ｂ０３５
	６６０		６６０Ａ　５Ｂ０４９
Ｇ０６Ｆ　12/00	５３７	Ｇ０６Ｆ　12/00	５３７Ｈ　５Ｂ０５８
12/14	３２０	12/14	３２０Ｆ　５Ｂ０８２

審査請求　未請求　請求項の数10　ＯＬ　（全 26 頁）　最終頁に続く

(21)出願番号　特願2000－348531(P2000－348531)

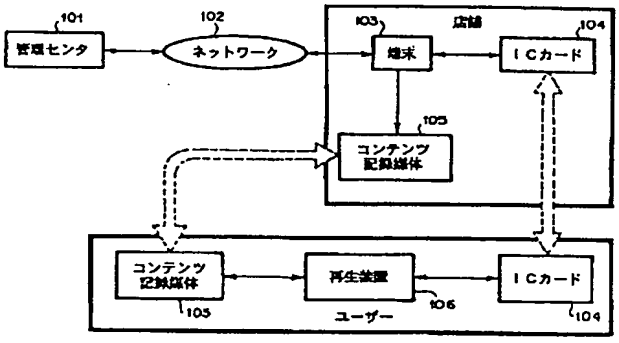
(22)出願日　平成12年11月15日(2000.11.15)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　太田　貢太郎
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　添田　修材
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100065385
弁理士　山下　穣平

最終頁に続く

(54)【発明の名称】　レンタルコンテンツ流通システムおよびその方法

(57)【要約】
【課題】　デジタルコンテンツの流通において、ユーザの利便性の向上と店舗の利益損失の解消と安全なコンテンツ保護を行う流通システムと流通方法を提供する。
【解決手段】　再生装置１０６とＩＣカードが相互認証し、ＩＣカードと管理センタ１０１が相互認証し、ＩＣカードは再生装置から受信した再生装置公開鍵証明書を管理センタに送信し、端末がコンテンツタイトルとレンタル期間を含む契約情報を使用者から入力し、これにＩＣカードによる署名を付したものを管理センタが受信し、管理センタがコンテンツ暗号鍵等を再生装置公開鍵等で暗号化して、署名して端末に送り、端末はそれをＩＣカードに書き込み、署名照合結果が正しければ、端末がコンテンツを記録媒体１０５に記録し、再生装置１０６は、ＩＣカードから受信する暗号化されたコンテンツ暗号鍵を復号し、それを用いてコンテンツを復号する。



【特許請求の範囲】

【請求項１】　再生装置公開鍵を含む再生装置公開鍵証明書を再生装置からＩＣカードへ送信し、ＩＣカード公開鍵を前記ＩＣカードから前記再生装置へ送信しつつ行われる、前記再生装置と前記ＩＣカードの間で相互認証を行うステップと、

ＩＣカード公開鍵を含むＩＣカード公開鍵証明書を前記ＩＣカードから管理センタへ送信しつつ行われる、前記ＩＣカードと管理センタとの間で端末を介して相互認証を行うステップと、

前記端末を介して前記ＩＣカードから前記再生装置公開鍵証明書を前記管理センタへ送信するステップと、

前記管理センタが、前記再生装置公開鍵証明書を認証するステップと、

前記端末が、契約情報を操作者から入力するステップと、

前記端末が、契約情報を前記ＩＣカードに送信するステップと、

前記ＩＣカードが、前記契約情報にＩＣカード秘密鍵により署名を付するステップと、

前記ＩＣカードが、前記ＩＣカード秘密鍵により署名が付された前記契約情報を前記端末を介して前記管理センタに送信するステップと、

前記管理センタが、前記契約情報を、前記契約情報に前記ＩＣカード秘密鍵により付された署名と照合するステップと、

前記管理センタが、前記契約情報中にあるコンテンツタイトルに対応するコンテンツ暗号鍵に管理センタ秘密鍵により署名を付するステップと、

前記管理センタが、前記管理センタ秘密鍵により署名が付された前記コンテンツ暗号鍵を前記再生装置公開鍵証明書中の再生装置公開鍵により暗号化するステップと、

前記管理センタが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により署名を付するステップと、

前記管理センタが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名を前記ＩＣカード公開鍵により暗号化するステップと、

前記管理センタが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ＩＣカード公開鍵により暗号化されたこれらのものを前記端末を介して前記ＩＣカードに送信するステップと、

前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ＩＣカード公開鍵により暗号化されたこれらのものより、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名を前記ＩＣカード秘密鍵により復号するステップと、

前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名と照合するステップと、

前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵を記憶するステップと、

前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名と照合する前記ステップの結果が正常であるときに、正常終了の旨を前記端末に送信するステップと、

前記端末が、前記正常終了の旨を前記ＩＣカードから受信したときに、前記コンテンツタイトルに対応するコンテンツデータであって前記コンテンツ暗号鍵により暗号化されているものを記録媒体に記録するステップと、

前記再生装置が、前記ＩＣカードに前記コンテンツ暗号鍵の要求を送信するステップと、

前記ＩＣカードが、前記再生装置から前記コンテンツ暗号鍵の要求を受信したときに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により署名を付するステップと、

前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信するステップと、

前記再生装置が、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により付された署名と照合するステップと、
前記再生装置が、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵より、前記コンテンツ暗号鍵及び前記コンテンツ暗号鍵に付された前記管理センタ秘密鍵による署名を再生装置秘密鍵により復号するステップと、
前記再生装置が、前記コンテンツ暗号鍵を、前記コンテンツ暗号鍵に付された前記管理センタ秘密鍵による署名と照合するステップと、
前記再生装置が、前記コンテンツ暗号鍵を記憶するステップと、
前記再生装置が、前記記録媒体に記録されている暗号化されている前記コンテンツデータより前記コンテンツ暗号鍵によりコンテンツデータを復号するステップと、
を有することを特徴とするレンタルコンテンツ流通方法。

【請求項２】　請求項１に記載のレンタルコンテンツ流通方法において、前記契約情報には契約期間が含まれ、
前記ＩＣカードが、前記契約情報中の契約期限を前記ＩＣカードのタイマにセットするステップと、
前記ＩＣカードが、前記再生装置から前記コンテンツ暗号鍵の要求を受信したときに、前記ＩＣカードのタイマからタイマ値を読み出すステップと、
を有し、
前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により署名を付する代わりに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記ＩＣカードのタイマから読み出されたタイマ値に前記ＩＣカード秘密鍵により署名を付し、
前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信する代わりに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記ＩＣカードのタイマから読み出されたタイマ値及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記ＩＣカードのタイマから読み出されたタイマ値に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信し、
前記再生装置が、前記再生装置のタイマに受信したタイマ値をセットするステップと、
前記ＩＣカードが、前記ＩＣカードのタイマの値が所定値になると、前記ＩＣカードが記憶する前記コンテンツ暗号鍵を消去するステップと、
前記再生装置が、前記再生装置のタイマの値が所定値になると、前記再生装置が記憶する前記コンテンツ暗号鍵を消去するステップと、
を有することを特徴とするレンタルコンテンツ流通方法。

【請求項３】　再生装置公開鍵を含む再生装置公開鍵証明書を再生装置からＩＣカードへ送信し、ＩＣカード公開鍵を前記ＩＣカードから受信しつつ、前記ＩＣカードの間で相互認証を行う手段と、
前記ＩＣカードにコンテンツ暗号鍵の要求を送信する手段と、
管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化されたコンテンツ暗号鍵を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵にＩＣカード秘密鍵により付された署名と照合する手段と、
前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵より、前記コンテンツ暗号鍵及び前記コンテンツ暗号鍵に付された前記管理センタ秘密鍵による署名を再生装置秘密鍵により復号する手段と、
前記コンテンツ暗号鍵を、前記コンテンツ暗号鍵に付された前記管理センタ秘密鍵による署名と照合する手段と、
前記コンテンツ暗号鍵を記憶する手段と、
記録媒体に記録されている暗号化されている前記コンテンツデータより前記コンテンツ暗号鍵によりコンテンツデータを復号する手段と、
を備えることを特徴とする再生装置。

【請求項４】　請求項３に記載の再生装置において、
前記契約情報には契約期間が含まれ、
受信したタイマ値が設置されるタイマと、
前記タイマの値が所定値になると、記憶する前記コンテンツ暗号鍵を消去する手段と、
を備えることを特徴とする再生装置。

【請求項５】　再生装置公開鍵を含む再生装置公開鍵証明書を再生装置から受信し、ＩＣカード公開鍵を前記再生装置へ送信しつつ、前記再生装置との間で相互認証を行う手段と、
ＩＣカード公開鍵を含むＩＣカード公開鍵証明書を管理センタへ送信しつつ、管理センタとの間で端末を介して相互認証を行う手段と、
前記端末を介して前記再生装置公開鍵証明書を前記管理センタへ送信する手段と、
前記端末から契約情報を受信する手段と、
前記契約情報にＩＣカード秘密鍵により署名を付する手

段と、
前記ＩＣカード秘密鍵により署名が付された前記契約情報を前記端末を介して前記管理センタに送信する手段と、
管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化されたコンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ＩＣカード公開鍵により暗号化されたこれらのものを前記端末を介して前記管理センタから受信する手段と、
前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ＩＣカード公開鍵により暗号化されたこれらのものより、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名を前記ＩＣカード秘密鍵により復号する手段と、
前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名と照合する手段と、
前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵を記憶する手段と、
前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名と照合する前記ステップの結果が正常であるときに、正常終了の旨を前記端末に送信する手段と、
前記再生装置から前記コンテンツ暗号鍵の要求を受信する手段と、
前記再生装置から前記コンテンツ暗号鍵の要求を受信したときに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により署名を付する手段と、
前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信する手段と、
を備えることを特徴とするＩＣカード。

【請求項６】　請求項５に記載のＩＣカードにおいて、
前記契約情報には契約期間が含まれ、
前記契約情報中の契約期限がセットされるタイマと、
前記再生装置から前記コンテンツ暗号鍵の要求を受信したときに、前記タイマからタイマ値を読み出す手段と、
前記タイマの値が所定値になると、記憶する前記コンテンツ暗号鍵を消去する手段と、
を備え、
前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により署名を付する手段の代わりに、
前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記ＩＣカードのタイマから読み出されたタイマ値に前記ＩＣカード秘密鍵により署名を付する手段を備え、
前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信する手段の代わりに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記ＩＣカードのタイマから読み出されたタイマ値及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記ＩＣカードのタイマから読み出されたタイマ値に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信する手段を備えることを特徴とするＩＣカード。

【請求項７】　ＩＣカード公開鍵を含むＩＣカード公開鍵証明書をＩＣカードから管理センタへ送信しつつ行われる前記ＩＣカードと管理センタとの間での相互認証に仲介する手段と、
前記ＩＣカードから前記管理センタへの前記再生装置公開鍵証明書の送信を仲介する手段と、
契約情報を操作者から入力する手段と、
前記契約情報を前記ＩＣカードに送信する手段と、
前記ＩＣカードから前記管理センタへのＩＣカード秘密鍵により署名が付された前記契約情報の送信を仲介する手段と、
前記管理センタから前記ＩＣカードへの管理センタ秘密鍵により署名が付され再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵に

より暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ＩＣカード公開鍵により暗号化されたこれらのものの送信を仲介する手段と、
前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名と照合した結果が正常であるときに、正常終了の旨を前記ＩＣカードから受信する手段と、
前記正常終了の旨を前記ＩＣカードから受信したときに、前記コンテンツタイトルに対応するコンテンツデータであって前記コンテンツ暗号鍵により暗号化されているものを記録媒体に記録する手段と、
を備えることを特徴とする端末。
【請求項８】　ＩＣカード公開鍵を含むＩＣカード公開鍵証明書をＩＣカードから受信しつつ、前記ＩＣカードとの間で端末を介して相互認証を行う手段と、
前記端末を介して前記ＩＣカードから再生装置公開鍵を含む再生装置公開鍵証明書を受信する手段と、
前記再生装置公開鍵証明書を認証する手段と、
前記ＩＣカードからＩＣカード秘密鍵により署名が付された契約情報を前記端末を介して受信する手段と、
前記契約情報を、前記契約情報に前記ＩＣカード秘密鍵により付された署名と照合する手段と、
前記契約情報中にあるコンテンツタイトルに対応するコンテンツ暗号鍵に管理センタ秘密鍵により署名を付する手段と、
前記管理センタ秘密鍵により署名が付された前記コンテンツ暗号鍵を前記再生装置公開鍵証明書中の再生装置公開鍵により暗号化する手段と、
前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により署名を付する手段と、
前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名を前記ＩＣカード公開鍵により暗号化する手段と、
前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ＩＣカード公開鍵により暗号化されたこれらのものを前記端末を介して前記ＩＣカードに送信する手段と、
を備えることを特徴とする管理センタ。
【請求項９】　請求項３に記載の再生装置と、請求項５に記載のＩＣカードと、請求項７に記載の端末と、請求項８に記載の管理センタを備えることを特徴とするレンタルコンテンツ流通システム。
【請求項１０】　請求項４に記載の再生装置と、請求項６に記載のＩＣカードと、請求項７に記載の端末と、請求項８に記載の管理センタを備えることを特徴とするレンタルコンテンツ流通システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、再生装置、再生情報記憶装置、管理センタ、コンテンツ流通システムにおいて、コンテンツ再生期限の管理、コンテンツを再生する再生装置の限定方法、コンテンツを再生する再生装置の機種の安全な変更方法に関する。
【０００２】
【従来の技術】第１の従来技術として、デジタルコンテンツのレンタルはビデオテープと同様にＤＶＤやＣＤを貸与しレンタル期間内に返却する方式がある。
【０００３】第２の従来技術として、ＤＶＤにはコンテンツの不正コピーを防止するためコンテンツデータを暗号化し媒体に記録され、暗号化したコンテンツデータを復号する鍵データも媒体に記録されている。
【０００４】第３の従来技術として、ＤＶＤ媒体へは暗号化されたコンテンツデータを記録し、復号する鍵データは電話回線等からインターネットを介して再生装置にダウンロードするには方式がある。
【０００５】
【発明が解決しようとする課題】しかしながら、この第１の従来技術による方法では、レンタルしたＤＶＤやＣＤをレンタル期間内に店舗に赴き返却しなければならず大変煩わしかった。
【０００６】また、レンタル期間を誤って超過しても追加料金を徴収されていた。
【０００７】さらに、レンタルした本人以外がコンテンツを再生するいわゆる見回し行為によってレンタル店に損失を与えていた。
【０００８】第２の従来技術による方法では、媒体には暗号化されたコンテンツデータを復号する鍵データを記録されているため、ハッカーによる不正な暗号の解読行為を防止することは不可能であり常に解読される脅威にさらされる。
【０００９】また昨今、ＤＶＤのライセンスを受けた企業であっても不手際により機密が漏洩し、暗号データが解読されており、機密情報の管理方法に問題があった。
【００１０】第３の従来技術による方法では、コンテンツ再生のためにユーザがプロバイダ契約や接続のための難解な設定を行う必要があり煩雑であった。

【００１１】本発明は、上記従来の問題点を鑑みなされたものであり、デジタルコンテンツの流通において、ユーザの利便性の向上と店舗の利益損失の解消と安全なコンテンツ保護を行う流通システムと流通方法を提供することを目的とする。

【００１２】

【課題を解決するための手段】本発明によるレンタルコンテンツ流通方法は、再生装置公開鍵を含む再生装置公開鍵証明書を再生装置からＩＣカードへ送信し、ＩＣカード公開鍵を前記ＩＣカードから前記再生装置へ送信しつつ行われる、前記再生装置と前記ＩＣカードの間で相互認証を行うステップと、ＩＣカード公開鍵を含むＩＣカード公開鍵証明書を前記ＩＣカードから管理センタへ送信しつつ行われる、前記ＩＣカードと管理センタとの間で端末を介して相互認証を行うステップと、前記端末を介して前記ＩＣカードから前記再生装置公開鍵証明書を前記管理センタへ送信するステップと、前記管理センタが、前記再生装置公開鍵証明書を認証するステップと、前記端末が、契約情報を操作者から入力するステップと、前記端末が、契約情報を前記ＩＣカードに送信するステップと、前記ＩＣカードが、前記契約情報にＩＣカード秘密鍵により署名を付するステップと、前記ＩＣカードが、前記ＩＣカード秘密鍵により署名が付された前記契約情報を前記端末を介して前記管理センタに送信するステップと、前記管理センタが、前記契約情報を、前記契約情報に前記ＩＣカード秘密鍵により付された署名と照合するステップと、前記管理センタが、前記契約情報中にあるコンテンツタイトルに対応するコンテンツ暗号鍵に管理センタ秘密鍵により署名を付するステップと、前記管理センタが、前記管理センタ秘密鍵により署名が付された前記コンテンツ暗号鍵を前記再生装置公開鍵証明書中の再生装置公開鍵により暗号化するステップと、前記管理センタが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により署名を付するステップと、前記管理センタが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名を前記ＩＣカード公開鍵により暗号化するステップと、前記管理センタが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ＩＣカード公開鍵により暗号化されたこれらのものを前記端末を介して前記ＩＣカードに送信するステップと、前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ＩＣカード公開鍵により暗号化されたこれらのものより、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名を前記ＩＣカード秘密鍵により復号するステップと、前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名と照合するステップと、前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵を記憶するステップと、前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名と照合する前記ステップの結果が正常であるときに、正常終了の旨を前記端末に送信するステップと、前記端末が、前記正常終了の旨を前記ＩＣカードから受信したときに、前記コンテンツタイトルに対応するコンテンツデータであって前記コンテンツ暗号鍵により暗号化されているものを記録媒体に記録するステップと、前記再生装置が、前記ＩＣカードに前記コンテンツ暗号鍵の要求を送信するステップと、前記ＩＣカードが、前記再生装置から前記コンテンツ暗号鍵の要求を受信したときに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により署名を付するステップと、前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信するステップと、前記再生装置が、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵に

より付された署名と照合するステップと、前記再生装置が、前記管理センタ秘密鍵により名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵より、前記コンテンツ暗号鍵及び前記コンテンツ暗号鍵に付された前記管理センタ秘密鍵による署名を再生装置秘密鍵により復号するステップと、前記再生装置が、前記コンテンツ暗号鍵を、前記コンテンツ暗号鍵に付された前記管理センタ秘密鍵による署名と照合するステップと、前記再生装置が、前記コンテンツ暗号鍵を記憶するステップと、前記再生装置が、前記記録媒体に記録されている暗号化されている前記コンテンツデータより前記コンテンツ暗号鍵によりコンテンツデータを復号するステップと、を有することを特徴とする。

【００１３】上記のレンタルコンテンツにおいて、前記契約情報には契約期間が含まれ、前記ＩＣカードが、前記契約情報中の契約期限を前記ＩＣカードのタイマにセットするステップと、前記ＩＣカードが、前記再生装置から前記コンテンツ暗号鍵の要求を受信したときに、前記ＩＣカードのタイマからタイマ値を読み出すステップと、を有し、前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により署名を付する代わりに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記ＩＣカードのタイマから読み出されたタイマ値に前記ＩＣカード秘密鍵により署名を付し、前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信する代わりに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記ＩＣカードのタイマから読み出されたタイマ値及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記ＩＣカードのタイマから読み出されたタイマ値に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信し、前記再生装置が、前記再生装置のタイマに受信したタイマ値をセットするステップと、前記ＩＣカードが、前記ＩＣカードのタイマの値が所定値になると、前記ＩＣカードが記憶する前記コンテンツ暗号鍵を消去するステップと、前記再生装置が、前記再生装置のタイマの値が所定値になると、前記再生装置が記憶する前記コンテンツ暗号鍵を消去するステップと、を有していてもよい。

【００１４】本発明による再生装置は、再生装置公開鍵を含む再生装置公開鍵証明書を再生装置からＩＣカードへ送信し、ＩＣカード公開鍵を前記ＩＣカードから受信しつつ、前記ＩＣカードの間で相互認証を行う手段と、前記ＩＣカードにコンテンツ暗号鍵の要求を送信する手段と、管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化されたコンテンツ暗号鍵を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵にＩＣカード秘密鍵により付された署名と照合する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵より、前記コンテンツ暗号鍵及び前記コンテンツ暗号鍵に付された前記管理センタ秘密鍵による署名を再生装置秘密鍵により復号する手段と、前記コンテンツ暗号鍵を、前記コンテンツ暗号鍵に付された前記管理センタ秘密鍵による署名と照合する手段と、前記コンテンツ暗号鍵を記憶する手段と、記録媒体に記録されている暗号化されている前記コンテンツデータより前記コンテンツ暗号鍵によりコンテンツデータを復号する手段と、を備えることを特徴とする。

【００１５】上記の再生装置において、前記契約情報には契約期間が含まれ、受信したタイマ値が設置されるタイマと、前記タイマの値が所定値になると、記憶する前記コンテンツ暗号鍵を消去する手段と、を備えていてもよい。

【００１６】本発明によるＩＣカードは、再生装置公開鍵を含む再生装置公開鍵証明書を再生装置から受信し、ＩＣカード公開鍵を前記再生装置へ送信しつつ、前記再生装置との間で相互認証を行う手段と、ＩＣカード公開鍵を含むＩＣカード公開鍵証明書を管理センタへ送信しつつ、管理センタとの間で端末を介して相互認証を行う手段と、前記端末を介して前記再生装置公開鍵証明書を前記管理センタへ送信する手段と、前記端末から契約情報を受信する手段と、前記契約情報にＩＣカード秘密鍵により署名を付する手段と、前記ＩＣカード秘密鍵により署名が付された前記契約情報を前記端末を介して前記管理センタに送信する手段と、管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化されたコンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ＩＣカード公開鍵により暗号化されたこれらのものを前記端末を介して前記管理センタから受信する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ＩＣカード公開鍵により暗号化されたこれらのものより、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ

秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名を前記ＩＣカード秘密鍵により復号する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名と照合する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵を記憶する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名と照合する前記ステップの結果が正常であるときに、正常終了の旨を前記端末に送信する手段と、前記再生装置から前記コンテンツ暗号鍵の要求を受信する手段と、前記再生装置から前記コンテンツ暗号鍵の要求を受信したときに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により署名を付する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信する手段と、を備えることを特徴とする。

【００１７】上記のＩＣカードにおいて、前記契約情報には契約期間が含まれ、前記契約情報中の契約期限がセットされるタイマと、前記再生装置から前記コンテンツ暗号鍵の要求を受信したときに、前記タイマからタイマ値を読み出す手段と、前記タイマの値が所定値になると、記憶する前記コンテンツ暗号鍵を消去する手段と、を備え、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により署名を付する手段の代わりに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記ＩＣカードのタイマから読み出されたタイマ値に前記ＩＣカード秘密鍵により署名を付する手段を備え、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信する手段の代わりに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記ＩＣカードのタイマから読み出されたタイマ値及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記ＩＣカードのタイマから読み出されたタイマ値に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信する手段を備えていてもよい。

【００１８】本発明による端末は、ＩＣカード公開鍵を含むＩＣカード公開鍵証明書をＩＣカードから管理センタへ送信しつつ行われる前記ＩＣカードと管理センタとの間での相互認証に仲介する手段と、前記ＩＣカードから前記管理センタへの前記再生装置公開鍵証明書の送信を仲介する手段と、契約情報を操作者から入力する手段と、前記契約情報を前記ＩＣカードに送信する手段と、前記ＩＣカードから前記管理センタへのＩＣカード秘密鍵により署名が付された前記契約情報の送信を仲介する手段と、前記管理センタから前記ＩＣカードへの管理センタ秘密鍵により署名が付され再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ＩＣカード公開鍵により暗号化されたこれらのものの送信を仲介する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名と照合した結果が正常であるときに、正常終了の旨を前記ＩＣカードから受信する手段と、前記正常終了の旨を前記ＩＣカードから受信したときに、前記コンテンツタイトルに対応するコンテンツデータであって前記コンテンツ暗号鍵により暗号化されているものを記録媒体に記録する手段と、を備えることを特徴とする。

【００１９】本発明による管理センタは、ＩＣカード公開鍵を含むＩＣカード公開鍵証明書をＩＣカードから受信しつつ、前記ＩＣカードとの間で端末を介して相互認証を行う手段と、前記端末を介して前記ＩＣカードから再生装置公開鍵を含む再生装置公開鍵証明書を受信する手段と、前記再生装置公開鍵証明書を認証する手段と、前記ＩＣカードからＩＣカード秘密鍵により署名が付された契約情報を前記端末を介して受信する手段と、前記契約情報を、前記契約情報に前記ＩＣカード秘密鍵により付された署名と照合する手段と、前記契約情報中にあるコンテンツタイトルに対応するコンテンツ暗号鍵に管理センタ秘密鍵により署名を付する手段と、前記管理センタ秘密鍵により署名が付された前記コンテンツ暗号鍵を前記再生装置公開鍵証明書中の再生装置公開鍵により暗号化する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コン

テンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により署名を付する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名を前記ＩＣカード公開鍵により暗号化する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ＩＣカード公開鍵により暗号化されたこれらのものを前記端末を介して前記ＩＣカードに送信する手段と、を備えることを特徴とする。

【００２０】本発明によるレンタルコンテンツ流通システムは、上記の再生装置と、上記のＩＣカードと、上記の端末と、上記の管理センタを備えることを特徴とする。

【００２１】

【発明の実施の形態】本発明の上記および他の目的、特徴および利点を明確にすべく、以下添付した図面を参照しながら、本発明の実施の形態につき詳細に説明する。

【００２２】図１を参照すると、本発明の一実施の形態としてのレンタルコンテンツ流通におけるシステムおよび流通方法の構成例が示されている。

【００２３】図１において、レンタルコンテンツ流通システムは、管理センタ１０１と、店舗に設置した端末１０３と、管理センタ１０１と端末１０３を結ぶネットワーク１０２と、ＩＣカード１０４とコンテンツ記録媒体１０５と、ユーザに設置されている再生装置１０６から構成される。

【００２４】図１において、管理センタ１０１は遠隔地に設置され、インターネット等のネットワーク１０２を介して店舗に設置している端末１０３と接続されている。なお図では省略しているが店舗は複数存在し、また１店舗に端末１０３が複数あっても良い。

【００２５】端末１０３にはユーザが持参したＩＣカード１０４とコンテンツ記録媒体１０５を接続する。

【００２６】再生装置１０６はユーザが所有しており、ユーザが所有しているＩＣカード１０４とコンテンツ記録媒体１０５を接続する。

【００２７】管理センタ１０１は複数のコンテンツ暗号鍵と、全ＩＣカードの公開鍵証明書と、全再生装置の公開鍵証明書と全ＩＣカードと全再生装置のペア情報を保管しており、端末１０３を介してＩＣカード１０４からＩＣカードの公開鍵証明書と再生装置の公開鍵証明書を受信し正当性を確認する。コンテンツ暗号鍵は、コンテンツ毎に異なり、それぞれのコンテンツ暗号鍵によりそれぞれのコンテンツが暗号化される。

【００２８】また端末１０３を介してＩＣカード１０４と相互認証した後、端末からの所定の手続きによりとコンテンツ暗号鍵とレンタル期間情報をＩＣカード１０４へ配信する。

【００２９】端末１０３には管理センタ１０１で保管しているコンテンツ暗号鍵で暗号化されたコンテンツが記録されており、ユーザは端末１０３によってコンテンツをレンタル購入するための操作を行う。

【００３０】端末１０３は管理センタ１０１とＩＣカード１０４との所定の手続きにより、コンテンツ記録媒体１０５に暗号化されたコンテンツをダウンロードする。

【００３１】ＩＣカード１０４は端末１０３を介して、コンテンツを暗号化したコンテンツ暗号鍵とレンタル期限情報をダウンロードし、レンタル期間中コンテンツ暗号鍵を保管し、レンタル期間を過ぎるとコンテンツ暗号鍵を消去する。

【００３２】また、ＩＣカードはユーザが所有している再生装置１０６との間で相互認証を行い、所定の手続きによりレンタル期間中はコンテンツ暗号鍵を再生装置１０６に配信する。

【００３３】コンテンツ記録媒体１０５は、管理センタ１０１とＩＣカード１０４の所定の手続きにより端末１０３に記録された暗号化されているコンテンツを記録する。また、コンテンツ記録媒体１０５はユーザが所有する再生装置１０６へ所定の手続き後、再生装置１０６の制御によりコンテンツデータが読み出される。

【００３４】ユーザが所有している再生装置１０６は、ＩＣカード１０４との認証処理後の所定の手続きによりＩＣカード１０４から送信されたコンテンツ暗号鍵をレンタル期間中まで保管し、レンタル期間が過ぎるかあるいは電源が切断されるまで保持する。

【００３５】また、再生装置１０６はコンテンツ記憶媒体１０５から暗号化されたコンテンツを所定の手続きにより読み出し、暗号化されたコンテンツデータをＩＣカード１０４から読み出したコンテンツ暗号鍵によって復号しレンタル期間中はコンテンツを再生する。

【００３６】図１の例の場合、順をおって説明する。

【００３７】まずＩＣカード１０１は前もって再生装置１０６と接続し、ＩＣカード１０４と再生装置１０６との間で相互認証を行う。ＩＣカード１０４は、相互認証の結果が正常であれば、再生装置公開鍵の証明書を記憶する。

【００３８】次にユーザはＩＣカード１０４とコンテンツ記録媒体１０５を店舗へ持参し端末１０３に接続する。

【００３９】端末１０３はＩＣカード１０４が接続されるとＩＣカード１０４からＩＣカード１０４の公開鍵証明書を読み出し、管理センタ１０１へ読み出したＩＣカード１０４の公開鍵証明書と共に相互認証の要求を行

う。

【００４０】管理センタ１０１はＩＣカード１０４の公開鍵証明書の有効性を確認し、ＩＣカード１０４との間で相互認証を行う。

【００４１】次に端末１０３は再生装置１０６の公開鍵証明書を読み出し、管理センタ１０１へ読み出した再生装置１０６の公開鍵証明書を転送する。

【００４２】管理センタ１０１は再生装置１０６の公開鍵証明書の有効性を確認する。

【００４３】次にユーザは端末１０３へレンタルするコンテンツのタイトルとレンタル期間を入力すると、端末１０３はＩＣカードへコンテンツのタイトルとレンタル期間を含む契約情報を送信し、ＩＣカード１０４から契約情報と契約情報へのＩＣカードの秘密鍵による署名を読み出す。

【００４４】端末１０３は管理センタ１０１に対してコンテンツ暗号鍵を要求するデータとして契約情報と契約情報への署名データを送信する。

【００４５】次に管理センタ１０１は、端末１０３からの契約情報と契約情報への署名を検証してデータの正当性が確認された場合、コンテンツタイトルに対応するコンテンツ暗号鍵を再生装置１０６の公開鍵を用いて暗号化し、その暗号化されたコンテンツ暗号鍵等とコンテンツ暗号鍵等への管理センターの秘密鍵による署名データをＩＣカード１０４へ端末１０３を介して送信する。

【００４６】ＩＣカード１０４は再生装置１０６の公開鍵によって暗号化されたコンテンツ暗号鍵と署名データを検証し、正当性が確認された場合、再生装置１０６の公開鍵によって暗号化されたコンテンツ暗号鍵をレンタル期間中のみ保管する。

【００４７】次に、端末１０３は、コンテンツタイトルに対応するコンテンツ暗号鍵によって既に暗号化されているコンテンツを所定の手順によりコンテンツ記録媒体１０５に転送し、ユーザは店舗にレンタル料金を支払い後、ＩＣカード１０４とコンテンツ記録媒体１０５を受け取る。

【００４８】次にユーザは所有の再生装置１０６へＩＣカード１０４とコンテンツ記録媒体１０５を接続する。

【００４９】再生装置１０６はＩＣカード１０４との間で相互認証し、正当性が確認できるとＩＣカード１０４からコンテンツ暗号鍵とコンテンツ暗号鍵への署名と契約情報等及び契約情報等への署名を読み取る。

【００５０】再生装置１０６はコンテンツ暗号鍵、契約情報と署名データを照合しデータの正当性が確認されると、再生装置１０６の公開鍵によって暗号化されているコンテンツ暗号鍵を再生装置１０６の秘密鍵で復号し、復号されたコンテンツ暗号鍵をレンタル期間あるいは電源が切断されるまで保管する。

【００５１】再生装置１０６はコンテンツ記憶媒体１０５から暗号されたコンテンツを読み出し、コンテンツ暗号鍵で復号しレンタル期間中あるいは電源が切断されるまでコンテンツを再生する。

【００５２】図２を参照すると、図１に示す管理センタ１０１の詳細な構成例が示されている。

【００５３】管理センタは制御部２０１、復号部２０２、暗号部２０３、圧縮部２０４、乱数発生部２０５、認証部２０６、通信部２０７、管理センタ秘密鍵記憶部２０８、管理センタ公開鍵記憶部２０９、コンテンツ暗号鍵記憶部２１０、公開鍵データベース２１１、課金情報データベース２１２を備える。

【００５４】管理センタ秘密鍵記憶部２０８には管理センタ１０１のみが所有する管理センタ秘密鍵が記録されている。

【００５５】管理センタ公開鍵記憶部２０９には管理センタ秘密鍵と所定の方法によりペアとなる管理センタ公開鍵が記録されている。

【００５６】コンテンツ暗号鍵記憶部２１０には、各コンテンツを暗号化するために用いられた各コンテンツ暗号鍵が記憶されている。各コンテンツ暗号鍵は、共通鍵である。

【００５７】公開鍵データベース２１１には、全ＩＣカードと全再生装置の公開鍵証明書と全ＩＣカードと全再生装置のペア情報（秘密鍵と公開鍵より成る情報）が記録されている。

【００５８】課金情報データベース２１２には、ユーザがレンタルしたコンテンツに関してのタイトルとレンタル期間とレンタル料金が記録されている。

【００５９】復号部２０２は通信部２０７を介して店舗の端末１０３からの暗号化データを受信すると制御部１０１の制御により、管理センタ秘密鍵記憶部２０８に記憶されている管理センタ秘密鍵、あるいは公開鍵データベース２１０に記録されたＩＣカードの公開鍵や再生装置の公開鍵を使って暗号データを復号する。

【００６０】暗号部２０３は、通信部２０７を介して店舗の端末１０３へデータを送信する時、制御部２０１の制御で管理センタ秘密鍵記憶部２０８に記憶している管理センタ秘密鍵あるいは公開鍵データベースに記録されたＩＣカードの公開鍵や再生装置の公開鍵を使いデータを暗号化する。

【００６１】圧縮部２０４はハッシュ関数を用いて制御部２０１の制御により任意のデータの圧縮を行う。

【００６２】乱数発生部２０５は制御部２０１の制御により乱数を発生する。

【００６３】認証部２０６は相互認証時に送信した乱数と受信した乱数の照合と、受信したデータと署名データの照合を行う。

【００６４】図３を参照すると、図１に示す端末１０３の詳細な構成例が示されている。

【００６５】端末１０３は、制御部３０１、通信部３０２、ＩＣカード入出力部３０３、コンテンツ記録媒体出

力部３０４、入力部３０５、表示部３０６、コンテンツ記憶部３０７から構成されている。

【００６６】通信部３０２は制御部３０１の制御によりインターネット等のネットワーク１０２を介して管理センタ１０１と通信を行う。

【００６７】ＩＣカード入出力部３０３は制御部３０１の制御によりＩＣカード１０４と通信する。

【００６８】コンテンツ記録媒体出力部３０４は制御部３０１の制御によりコンテンツ記録媒体１０５へコンテンツ記憶部３０７のコンテンツデータを出力する。

【００６９】入力部３０５はレンタルするコンテンツの選択とレンタル期間をユーザが操作し入力するためのユーザインターフェースである。

【００７０】表示部３０６はレンタルするコンテンツのタイトル表示とレンタル期間を表示するユーザインターフェースである。

【００７１】コンテンツ記憶部３０７には、暗号化されたコンテンツが記憶されている。

【００７２】図４を参照すると、図１に示すＩＣカード１０４の詳細な構成例が示されている。

【００７３】ＩＣカードは制御部４０１、入出力部４０２、復号部４０３、暗号部４０４、圧縮部４０５、乱数発生部４０６、認証部４０７、ＩＣカード秘密鍵記憶部４０８、管理センタ公開鍵記憶部４０９、ＩＣカード公開鍵証明書記憶部４１０、再生装置公開鍵証明書記憶部４１１、コンテンツ暗号鍵記憶部４１２、タイマ４１３、電池４１４から構成される。

【００７４】ＩＣカード秘密鍵記憶部４０８には、ＩＣカードの秘密鍵が記憶されている。

【００７５】管理センタ公開鍵記憶部４０９は、管理センタの公開鍵が記憶されている。

【００７６】ＩＣカード公開鍵証明書記憶部４１０は、管理センタ１０１が発行したＩＣカード公開鍵証明書が記憶される。

【００７７】再生装置公開鍵証明書記憶部４１１には、管理センタ１０１が発行した再生装置公開鍵証明書であって再生装置１０６から読み出されたものが記憶される。

【００７８】コンテンツ暗号鍵記憶部４１２は電池４１４でバックアップされており、管理センタ１０１から配布を受ける暗号化されたコンテンツ暗号鍵をタイマ４１３が所定の値に変化するまで記憶する。

【００７９】タイマ４１３は電池４１４でバックアップされており、管理センタ１０１から配布されたタイマの初期値から時間と共に変化し所定の値になるとコンテンツ暗号鍵記憶部４１２に記憶されているコンテンツ暗号鍵を消去する。

【００８０】復号部４０３は入出力部４０２を介して店舗の端末１０３あるいはユーザが所有する再生装置１０６からの暗号化データを受信すると制御部４０１の制御により、ＩＣカード秘密鍵、あるいは管理センタ公開鍵を使って暗号化データを復号する。

【００８１】暗号部４０４は、入出力部４０２を介して店舗の端末１０３あるいはユーザが所有する再生装置１０６へデータを送信する時、制御部１０１の制御によりＩＣカード秘密鍵あるいは再生装置の公開鍵を使いデータを暗号化する。

【００８２】圧縮部４０５はハッシュ関数を用いて制御部４０１の制御により任意のデータの圧縮を行う。

【００８３】乱数発生部４０６は制御部４０１の制御により乱数を発生する。

【００８４】認証部４０７は相互認証時に送信した乱数と受信した乱数の照合と、受信したデータと署名データの照合を行う。

【００８５】図５を参照すると、図１に示す再生装置１０６の詳細な構成例が示されている。

【００８６】再生装置１０６は制御部５０１と、ＩＣカード入出力部５０２と、復号部５０３と、暗号部５０４と、圧縮部５０５と、乱数発生部５０６と、認証部５０７と、操作入力部５０８と、コンテンツ記録媒体入出力部５０９と、再生装置秘密鍵記憶部５１０と、管理センタ公開鍵記憶部５１１と、再生装置公開鍵証明書記憶部５１２と、タイマ５１３と、コンテンツ暗号鍵記憶部５１４と、コンテンツ暗号鍵復号部５１５と、コンテンツ再生部５１６とで構成されている。

【００８７】再生装置秘密鍵記憶部５１０には、再生装置１０６の秘密鍵が記憶されている。

【００８８】管理センタ公開鍵記憶部５１１は、管理センタ公開鍵が記憶されている。

【００８９】再生装置公開鍵証明書記憶部５１２には管理センタ１０１が発行した再生装置公開鍵証明書が記憶されている。

【００９０】タイマ５１３には、ＩＣカード入出力部５０２を介してＩＣカード１０４から読み出されたレンタル期間を示す所定のタイマ値が制御部５０１により書き込まれる。タイマ５１３のタイマ値は時間と共に変化し、タイマ５１３は、タイマ５１３のタイマ値がレンタル期間が終了する所定の値になるとコンテンツ暗号鍵記憶部５１４に記憶されているコンテンツ暗号鍵をクリアする。

【００９１】コンテンツ暗号鍵記憶部５１４には、制御部５０１がＩＣカード入出力部５０２介してＩＣカード１０４から読み出した暗号化されたコンテンツ暗号鍵が記憶される。

【００９２】復号部５０３はＩＣカード入出力部５０２を介してＩＣカード１０４から暗号化データやデジタル署名データを受信すると制御部５０１の制御により、再生装置秘密鍵、あるいは管理センタ公開鍵を使って暗号化データやデジタル署名データを復号する。

【００９３】暗号部５０４はＩＣカード入出力部５０２

を介してＩＣカード１０４へデータを送信する時、制御部１０１の制御により再生装置秘密鍵を使いデータを暗号化する。

【００９４】圧縮部５０５はハッシュ関数を用いて制御部５０１の制御により任意のデータの圧縮を行う。

【００９５】乱数発生部５０６は制御部５０１の制御により乱数を発生する。

【００９６】認証部５０７は相互認証時に送信した乱数と受信した乱数の照合と、受信したデータと署名データの照合を行う。

【００９７】次に図１の再生装置１０６とＩＣカード１０４の相互認証の動作を図６に示すタイムチャートを使用して順に説明する。

【００９８】この相互認証はＩＣカード１０４と再生装置１０６の工場出荷前、ユーザが本システムを初めて利用する時、再生装置１０６の機種変更時、及びコンテンツ再生時に行われる。

【００９９】まず、再生装置１０６へＩＣカード１０４を接続する（Ｓ１０１）。

【０１００】再生装置１０６の制御部５０１はＩＣカード入出力部５０２を介してＩＣカード１０４の接続を確認し、認識されるまで処理を繰り返す（Ｓ１０２）。

【０１０１】再生装置１０６の制御部５０１はＩＣカード入出力部５０２を介してＩＣカード１０４の接続を確認すると、ＩＣカード１０４に対して再生装置公開鍵証明書記憶部５１２に記憶されている再生装置公開鍵証明書（ＰＫｐｌ，Ｓ１）と共に相互認証の要求をＩＣカード入出力部５０２を介して行う（Ｓ１０３）。

【０１０２】次に、ＩＣカード１０４の制御部４０１は入出力部４０２を介して再生装置公開鍵証明書ＰＫｐｌ，Ｓ１と共に相互認証の要求を受信すると、管理センタ公開鍵記憶部４０９に記憶されている管理センタ公開鍵ＰＫｃｎｔを用いて再生装置公開鍵証明書の署名Ｓ１を復号部４０３にて復号しＰＫｃｎｔ（Ｓ１）を生成し、圧縮部４０５にてハッシュ関数を用いて再生装置公開鍵ＰＫｐｌを圧縮しＨ（ＰＫｐｌ）を生成し、認証部４０７にてＰＫｃｎｔ（Ｓ１）とＨ（ＰＫｐｌ）を照合する（Ｓ１０４）。

【０１０３】Ｓ１０５においてＰＫｃｎｔ（Ｓ１）とＨ（ＰＫｐｌ）が不一致である場合、ＩＣカード１０４の制御部４０１は再生装置１０６から受信した再生装置公開鍵証明書を管理センタ１０１が発行していない不正な再生装置公開鍵証明書であると判断し、入出力部４０２を介して再生装置１０６へエラー通知を行う（Ｓ１０６）。

【０１０４】再生装置１０６の制御部５０１はＩＣカード入出力部５０２を介してエラー通知を受信すると（Ｓ１０７）、相互認証を中止する（Ｓ１３０）。

【０１０５】Ｓ１０５においてＰＫｃｎｔ（Ｓ１）とＨ（ＰＫｐｌ）が一致した場合、ＩＣカード１０４の制御部４０１は再生装置１０６から受信した再生装置公開鍵証明書を管理センタ１０１が発行した正当な再生装置公開鍵証明書である判断し、ＩＣカード公開鍵証明書記憶部４１０に記憶されているＩＣカード公開鍵証明書（ＰＫｉｃ．Ｓ２）を再生装置１０６へ入出力部４０２を介して送信する（Ｓ１０８）。

【０１０６】再生装置１０６の制御部５０１はＩＣカード入出力部５０２を介してＩＣカード公開鍵証明書（ＰＫｉｃ．Ｓ２）を受信すると、管理センタ公開鍵記憶部５１１に記憶している管理センタ公開鍵ＰＫｃｎｔを用いて署名Ｓ２を復号部５０３にて復号しＰＫｃｎｔ（Ｓ２）を生成し、圧縮部５０５にてハッシュ関数を用いてＩＣカード公開鍵ＰＫｉｃを圧縮しＨ（ＰＫｉｃ）を生成し、認証部５０７にてＰＫｃｎｔ（Ｓ２）とＨ（ＰＫｉｃ）を照合する（Ｓ１０９）。

【０１０７】Ｓ１１０において、ＰＫｃｎｔ（Ｓ２）とＨ（ＰＫｉｃ）が不一致である場合、再生装置１０６の制御部５０１は、ＩＣカード１０４から受信したＩＣカード公開鍵証明書が管理センタ１０１が発行していない不正なＩＣカード公開鍵証明書であると判断し相互認証を中止する（Ｓ１３０）。

【０１０８】Ｓ１１０において、ＰＫｃｎｔ（Ｓ２）とＨ（ＰＫｉｃ）が一致した場合、再生装置１０６の制御部５０１は、ＩＣカード１０４から受信したＩＣカード公開鍵証明書を管理センタ１０１が発行した正当なＩＣカード公開鍵証明書であると判断し、次に乱数発生部５０６で乱数Ｒｐｌを生成する（Ｓ１１１）。

【０１０９】再生装置１０６の制御部５０１はＩＣカード公開鍵ＰＫｉｃを用いて乱数Ｒｐｌを暗号部５０４にて暗号化しＰＫｉｃ（Ｒｐｌ）を生成し（Ｓ１１２）、ＰＫｉｃ（Ｒｐｌ）をＩＣカード１０４へＩＣカード入出力部５０２を介して送信する（Ｓ１１３）。

【０１１０】ＩＣカード１０４の制御部４０１は入出力部４０２を介してＰＫｉｃ（Ｒｐｌ）を受信すると、ＩＣカード秘密鍵記憶部４０８に記憶しているＩＣカード秘密鍵ＳＫｉｃを用いてＰＫｉｃ（Ｒｐｌ）を復号部４０３にて復号しＤＲｐｌを生成する（Ｓ１１４）。

【０１１１】次に乱数発生部４０６で乱数Ｒｉｃを生成し（Ｓ１１５）、再生装置公開鍵ＰＫｐｌを用いて乱数Ｒｉｃを暗号部４０４にて暗号化しＰＫｐｌ（Ｒｉｃ）を生成し（Ｓ１１６）、ＰＫｐｌ（Ｒｉｃ）とＤＲｐｌを入出力部４０２を介して再生装置１０６へ送信する（Ｓ１１７）。

【０１１２】再生装置１０６の制御部５０１はＩＣカード入出力部５０２からＰＫｐｌ（Ｒｉｃ）とＤＲｐｌを受信すると（Ｓ１１８）、再生装置１０６がステップＳ１１１で生成した乱数ＲｐｌとＩＣカード１０４がステップＳ１１４で復号したＤＲｐｌを認証部５０７で照合する（Ｓ１１９）。

【０１１３】Ｓ１１９において、ＲｐｌとＤＲｐｌが不

一致である場合、再生装置１０６の制御部５０１は、ＩＣカード１０４がＩＣカード１０４から受信してあるＩＣカード公開鍵とペアではないＩＣカード秘密鍵を保持した不正なＩＣカードである判断し相互認証を中止する（Ｓ１３０）。

【０１１４】Ｓ１１９において、ＲｐｌとＤＲｐｌが一致した場合、再生装置１０６の制御部５０１は、ＩＣカード１０４がＩＣカード１０４から受信してあるＩＣカード公開鍵とペアであるＩＣカード秘密鍵を保持した正当なＩＣカードであると判断し、再生装置秘密鍵記憶部５１０に記憶されている再生装置秘密鍵ＳＫｐｌを用いてＳ１１８にて受信したＰＫｐｌ（Ｒｉｃ）を復号部５０３で復号しＤＲｉｃを生成し（Ｓ１２０）、ＩＣカード入出力部５０２を介してＩＣカード１０４へＤＲｉｃを送信する（Ｓ１２１）。

【０１１５】ＩＣカード１０４の制御部４０１は入出力部４０２からＤＲｉｃを受信すると（Ｓ１２２）、ＩＣカード１０４がステップＳ１１５で生成した乱数ＲｉｃとＲｉｃと再生装置１０６がステップＳ１２０で復号したＤＲｉｃを認証部４０７で照合する（Ｓ１２３）。

【０１１６】Ｓ１２３において、ＲｉｃとＤＲｉｃが不一致である場合、ＩＣカード１０４の制御部４０１は入出力部４０２を介して再生装置１０６へエラー通知を行う（Ｓ１２４）。

【０１１７】再生装置１０６の制御部５０１はＩＣカード入出力部５０２からエラー通知を受信すると（Ｓ１２５）、相互認証を中止する（Ｓ１３０）。

【０１１８】Ｓ１２３において、ＲｉｃとＤＲｉｃが一致した場合、ＩＣカード１０４の制御部４０１は再生装置公開鍵証明書記憶部４１１の内容と、Ｓ１０４で受信した再生装置公開鍵証明書（ＰＫｐｌ．Ｓ）を比較する（Ｓ１２６）。

【０１１９】Ｓ１２６において、再生装置公開鍵証明書記憶部４１１の内容と、Ｓ１０４で受信した再生装置公開鍵証明書（ＰＫｐｌ．Ｓ）が異なる場合、Ｓ１０４で受信した再生装置１０６の公開鍵証明書（ＰＫｐｌ．Ｓ）を再生装置公開鍵証明書記憶部４１１に記憶する（Ｓ１２７）。

【０１２０】Ｓ１２６において、再生装置公開鍵証明書記憶部４１１の内容と、Ｓ１０４で受信した再生装置公開鍵証明書（ＰＫｐｌ．Ｓ）が等しい場合、Ｓ１２８へ遷移する。

【０１２１】次にＩＣカード１０４の制御部４０１は相互認証の正常終了を入出力部４０２を介して再生装置１０６へ通知し（Ｓ１２８）、再生装置１０６の制御部５０１はＩＣカード入出力部５０２を介して相互認証の正常終了を受信すると相互認証を終了する（Ｓ１２９）。

【０１２２】次に図１に示すＩＣカード１０４と管理センタ１０１の相互認証の動作を図７に示すタイムチャートを使用して説明する。

【０１２３】ユーザはＩＣカード１０４とコンテンツ記録媒体１０５を店舗の端末１０３へ持参しＩＣカード１０４とコンテンツ記録媒体１０５を端末１０３へ接続する（Ｓ２０１）。

【０１２４】端末１０３の制御部３０１はＩＣカード入出力部３０３を介してＩＣカード１０４の接続を確認すると（Ｓ２０２）、ＩＣカード１０４の相互認証を実施するため、制御部３０１はＩＣカード公開鍵証明書の読み出し要求をＩＣカード入出力部３０３を介してＩＣカード１０４へ通知する（Ｓ２０３）。

【０１２５】ＩＣカード１０４の制御部４０１は入出力部４０２からＩＣカード１０４の公開鍵証明書の読み出し要求を受信すると、ＩＣカード公開鍵証明書記憶部４１０に記憶されているＩＣカード公開鍵証明書（ＰＫｉｃ，Ｓ２）を入出力部４０２を介して端末１０３へ送信する（Ｓ２０４）。

【０１２６】次に、端末１０３の制御部３０１はＩＣカード入出力部３０３からＩＣカード公開鍵証明書（ＰＫｉｃ，Ｓ２）を受信すると、通信部３０２からネットワーク１０２を介して管理センタ１０１へＩＣカード公開鍵証明書（ＰＫｉｃ．Ｓ２）と共に相互認証を要求する（Ｓ２０５）。

【０１２７】管理センタ１０１の制御部２０１は通信部２０７を介して端末１０３からの相互認証要求とＩＣカード公開鍵証明書（ＰＫｉｃ．Ｓ２）を受信すると（Ｓ２０６）、公開鍵データベース２１１からＩＣカード公開鍵証明書（ＰＫｉｃ．Ｓ２）中のＩＣカード公開鍵ＰＫｉｃと同一のＩＣカード公開鍵を検索しＩＣカード公開鍵ＰＫｉｃが有効であるか確認する（Ｓ２０７）。

【０１２８】Ｓ２０７において、ＩＣカード公開鍵ＰＫｉｃが不正あるいは失効している場合、管理センタ１０１の制御部２０１は相互認証要求の応答として通信部２０７からネットワーク１０２を介して端末１０３へエラー通知を送信し（Ｓ２０８）、端末１０３の制御部３０１は通信部３０２を介してＳ２０８のエラー通知を受信すると相互認証処理を中止する（Ｓ２３０）。

【０１２９】Ｓ２０７によりＩＣカード公開鍵ＰＫｉｃが有効であると判断した場合、Ｓ２０６で受信したＩＣカード公開鍵証明書（ＰＫｉｃ．Ｓ２）の署名Ｓ２を管理センタ公開鍵記憶部２０９に記憶されている管理センタ公開鍵ＰＫｃｎｔを用いて復号部２０３にて復号しＰＫｃｎｔ（Ｓ２）を生成し、ＰＫｉｃを圧縮部２０４にてハッシュ関数を用いて圧縮しＨ（ＰＫｉｃ）を生成し、次に認証部２０６にてＰＫｃｎｔ（Ｓ２）とＨ（ＰＫｉｃ）が等しいか照合する（Ｓ２０８）。

【０１３０】Ｓ２０９において、ＰＫｃｎｔ（Ｓ２）とＨ（ＰＫｉｃ）が不一致の場合、管理センタ１０１の制御部２０１は、ステップＳ２０６で受信した公開鍵証明書（ＰＫｉｃ．Ｓ２）が管理センタ１０１が発行していない公開鍵証明書であると判断して通信部２０７からネ

ットワーク１０２を介して端末１０３へエラーを通知し（Ｓ２１０）、端末１０３の制御部３０１はＳ２１０より通信部３０２を介してエラー通知を受信すると相互認証を中止する（Ｓ２３０）。

【０１３１】Ｓ２０９において、ＰＫｃｎｔ（Ｓ２）とＨ（ＰＫｉｃ）が一致した場合、管理センタ１０１の制御部２０１は、Ｓ２０６で受信したＩＣカード公開鍵証明書（ＰＫｉｃ，Ｓ２）が管理センタ１０１が発行した公開鍵証明書であると判断して乱数発生部２０５で乱数Ｒｃｎｔを発生させ（Ｓ２１１）、ＩＣカード公開鍵ＰＫｉｃを用いて暗号部２０３にて乱数Ｒｃｎｔを暗号化しＰＫｉｃ（Ｒｃｎｔ）を生成し（Ｓ２１２）、通信部２０７からネットワーク１０２を介して端末１０３へ相互認証要求の応答データとしてＰＫｉｃ（Ｒｃｎｔ）を送信する（Ｓ２１３）。

【０１３２】端末１０３の制御部３０１は、通信部３０２から暗号データＰＫｉｃ（Ｒｃｎｔ）を受信すると、ＩＣカード入出力部３０３を介してＩＣカード１０４へＰＫｉｃ（Ｒｃｎｔ）を送信する（Ｓ２１４）。

【０１３３】ＩＣカード１０４の制御部４０１は、入出力部４０２からはＰＫｉｃ（Ｒｃｎｔ）を受信すると、復号部４０３にてＩＣカード秘密鍵記憶部４０８に記憶されているＩＣカード秘密鍵ＳＫｉｃを用いてＰＫｉｃ（Ｒｃｎｔ）を復号部４０３で復号しＤＲｃｎｔを生成する（Ｓ２１５）。

【０１３４】次にＩＣカード１０４の制御部４０１は乱数発生部４０６にて乱数Ｒｉｃを発生し（Ｓ２１６）、暗号部４０４にて管理センタ公開鍵記憶部４０９に記憶されている管理センタ公開鍵ＰＫｃｎｔを用いて暗号部４０４で暗号化しＰＫｃｎｔ（Ｒｉｃ）を生成し（Ｓ２１７）、相互認証要求の応答データとしてＰＫｃｎｔ（Ｒｉｃ）とＤＲｃｎｔを入出力部４０２から端末１０３へ送信する（Ｓ２１８）。

【０１３５】端末１０３の制御部３０１はＩＣカード入出力部３０３からＰＫｃｎｔ（Ｒｉｃ）とＤＲｃｎｔを受信すると、管理センタ１０１へ相互認証要求の応答データとして通信部３０２からネットワーク１０２を介してＰＫｃｎｔ（Ｒｉｃ）とＤＲｃｎｔを送信する（Ｓ２１９）。

【０１３６】管理センタ１０１の制御部２０１は通信部２０７からＰＫｃｎｔ（Ｒｉｃ）とＤＲｃｎｔを受信すると（Ｓ２２０）、認証部２０６にて復号データＤＲｃｎｔとステップ２１１で発生した乱数データＲｃｎｔを照合する（Ｓ２２１）。

【０１３７】Ｓ２２１において、ＤＲｃｎｔとＲｃｎｔが不一致である場合、管理センタ１０１の制御部２０１は、ＩＣカード１０４がＩＣカード公開鍵ＰＫｉｃのペアであるＩＣカード秘密鍵を保持していない不正なＩＣカードと判断し、通信部２０７からネットワーク１０２を介して端末１０３へエラー通知し（Ｓ２２２）、端末１０３の制御部３０１は通信部３０２からエラー通知を受信すると相互認証を中止する（Ｓ２３０）。

【０１３８】Ｓ２２１において、ＤＲｃｎｔとＲｃｎｔが一致する場合、管理センタ１０１の制御部２０１は、ＩＣカード１０４がＩＣカード公開鍵ＰＫｉｃのペアであるＩＣカード秘密鍵を保持している正当なＩＣカードであると判断し、復号部２０２にて管理センタ秘密鍵記憶部２０８に記憶している管理センタ秘密鍵ＳＫｃｎｔを用いてＰＫｃｎｔ（Ｒｉｃ）を復号しＤＲｉｃを生成し通信部２０７からネットワーク１０２を介して端末１０３へＤＲｉｃを送信する（Ｓ２２３）。

【０１３９】端末１０３の制御部３０１は通信部３０２からＤＲｉｃを受信すると、ＩＣカード入出力部３０３を介してＩＣカード１０４へＤＲｉｃを送信する（Ｓ２２４）。

【０１４０】次にＩＣカード１０４の制御部４０１は入出力部４０２を介して端末１０３からＤＲｉｃを受信すると（Ｓ２２５）、ステップＳ２１６で発生した乱数ＲｉｃとＤＲｉｃを認証部４０７にて照合する（Ｓ２２６）。

【０１４１】Ｓ２２６において、乱数ＲｉｃとＤＲｉｃが不一致である場合、ＩＣカード１０４の制御部４０１は、管理センタ１０１が管理センタ秘密鍵ＳＫｃｎｔを保持していない不正な相手と判断し、入出力部４０２から端末１０３へエラー通知し（Ｓ２２７）、端末１０３の制御部３０１はＩＣカード入出力部３０３からエラー通知を受信すると相互認証を中止する。

【０１４２】Ｓ２２６において、Ｒｉｃと復号データＤＲｉｃが一致した場合、ＩＣカード１０４の制御部４０１は、管理センタ１０１が管理センタ秘密鍵ＳＫｃｎｔを保持している正当な管理センタであると判断し、入出力部４０２から端末１０３へ正常終了の通知を送信し（Ｓ２２８）、端末１０３の制御部３０１はＩＣカード入出力部３０３から正常終了の通知を受信すると相互認証を正常終了する（Ｓ２２９）。

【０１４３】図８は、上記のＩＣカード１０４と管理センタ１０１の相互認証終了後のＩＣカード１０４から管理センタ１０１への再生装置公開鍵証明書の転送処理を示している。

【０１４４】まず端末１０３の制御部３０１はＩＣカード入出力部３０３からＩＣカード１０４へ再生装置公開鍵証明書の読み出し要求する（Ｓ３０１）。

【０１４５】ＩＣカード１０４の制御部４０１は入出力部４０２を介して端末１０３から再生装置公開鍵証明書の読み出し要求を受信すると、再生装置公開証明書記憶部４１１に記憶している再生装置公開鍵証明書（ＰＫｐｌ，Ｓ１）を入出力部４０２から端末１０３へ送信する（Ｓ３０２）。

【０１４６】端末１０３の制御部３０１はＩＣカード入出力部３０３から再生装置公開鍵証明書（ＰＫｐｌ，Ｓ

1）を受信すると、通信部３０２からネットワーク１０２を介して管理センタ１０１へ再生装置公開鍵証明書（ＰＫｐｌ，Ｓ1）を送信する（Ｓ３０４）。

【０１４７】管理センタ１０１の制御部２０１は通信部２０７を介して端末１０３から再生装置公開鍵証明書（ＰＫｐｌ，Ｓ1）を受信すると（Ｓ３０５）、再生装置公開鍵証明書（ＰＫｐｌ，Ｓ1）中の公開鍵ＰＫｐｌと同一の公開鍵を公開鍵データベース２１１から検索し、その公開鍵が有効な公開鍵であるか検証する（Ｓ３０６）。

【０１４８】Ｓ３０６において、Ｓ３０５で受信した再生装置公開鍵証明書が不正あるいは失効している場合、管理センタ１０１の制御部２０１は通信部２０７からネットワークを介して端末１０３へエラー通知をし（Ｓ３０７）、端末１０３の制御部３０１は通信部３０２からエラー通知を受信すると再生装置公開鍵証明書の転送処理を中止する（Ｓ３１３）。

【０１４９】Ｓ３０６において、Ｓ３０５で受信した再生装置公開鍵証明書が正当であると判断した場合、管理センタ公開鍵記憶部２０９に記憶している管理センタ公開鍵ＰＫｃｎｔを用いて再生装置公開鍵証明書（ＰＫｐｌ，Ｓ1）中の署名Ｓ1を復号部２０２で復号しＰＫｃｎｔ（Ｓ1）を生成し、ハッシュ関数を用いて再生装置公開鍵証明書（ＰＫｐｌ，Ｓ1）中のＰＫｐｌを圧縮部２０４で圧縮しＨ（ＰＫｐｌ）を生成し、ＰＫｃｎｔ（Ｓ1）とＨ（ＰＫｐｌ）を認証部２０６にて照合する（Ｓ３０８）。

【０１５０】Ｓ3.09において、ＰＫｃｎｔ（Ｓ1）とＨ（ＰＫｐｌ）が不一致である場合、管理センタ１０１の制御部２０１は、再生装置１０６が再生装置公開鍵ＰＫｐｌとペアである再生装置秘密鍵ＳＫｐｌを保持しない不正な再生装置であると判断し、通信部２０７からネットワーク１０２を介して端末１０３へエラー通知を送信し（Ｓ３１０）、端末１０３の制御部３０１は通信部３０２からエラー通知を受信すると再生装置公開鍵証明書の転送処理を中止する（Ｓ３１３）。

【０１５１】Ｓ３０９において、ＰＫｃｎｔ（Ｓ1）とＨ（ＰＫｐｌ）が一致した場合、管理センタ１０１の制御部２０１は、再生装置１０６が再生装置公開鍵ＰＫｐｌとペアである再生装置秘密鍵ＳＫｐｌを保持した正当な再生装置であると判断し、通信部２０２からネットワーク１０２を介して端末１０３へ正常終了通知し（Ｓ３１１）、端末１０３の制御部３０１は通信部３０２から正常終了の通知を受信すると再生装置公開鍵証明書の転送処理を正常終了する（Ｓ３１２）。

【０１５２】図9は、上記の再生装置公開鍵証明書の転送処理の後に行われるコンテンツの再生に必要な情報のダウンロード処理のタイムチャートを示している。

【０１５３】まず、ユーザは端末１０３の表示部３０６からレンタルするコンテンツを選択し、入力部３０５にてコンテンツのタイトルＣとレンタル期間Ｔを入力する（Ｓ４０１）。

【０１５４】コンテンツのタイトルＣとレンタル期間Ｔを含む契約内容を契約情報ＣＴとして、端末１０３の制御部３０１は契約情報ＣＴと共に契約データ作成要求をＩＣカード入出力部３０３を介してＩＣカード１０４へ送信する（Ｓ４０２）。

【０１５５】ＩＣカード１０４の制御部４０１は入出力部４０２から契約データ作成要求と契約情報ＣＴを受信すると、契約情報ＣＴを圧縮部４０５にてハッシュ関数を用いて圧縮しＨ（ＣＴ）を生成し、ＩＣカード秘密鍵記憶部４０８に記憶しているＩＣカード秘密鍵ＳＫｉｃを用いてＨ（ＣＴ）を暗号部４０４で暗号化することにより契約情報へのＩＣカード秘密鍵による署名Ｓ３を生成する（Ｓ４０３）。

【０１５６】次にＩＣカード１０４の制御部４０１は、入出力部４０２を介して契約情報ＣＴと署名Ｓ３を端末１０３へ送信する（Ｓ４０４）。

【０１５７】端末１０３の制御部３０１はＩＣカード入出力部３０３から契約情報ＣＴと署名Ｓ３を受信すると、通信部３０２からネットワーク１０２を介して管理センタ１０１へ契約情報ＣＴと署名Ｓ３と共にコンテンツ暗号鍵のダウンロード要求を送信する（Ｓ４０５）。

【０１５８】管理センタ１０１の制御部２０１は通信部２０７からコンテンツ暗号鍵ダウンロード要求と契約情報ＣＴと署名Ｓ３を受信すると（Ｓ４０６）、上記の相互認証によって正常と確認されたＩＣカードの公開鍵ＰＫｉｃを用いてＳ３を復号部２０２で復号しＰＫｉｃ（Ｓ３）を生成し、圧縮部２０４にてハッシュ関数を用いて契約情報ＣＴを圧縮しＨ（ＣＴ）を生成し、認証部２０６にてＰＫｉｃ（Ｓ３）とＨ（ＣＴ）を照合する（Ｓ４０７）。

【０１５９】Ｓ４０８において、ＰＫｉｃ（Ｓ３）とＨ（ＣＴ）が不一致である場合、管理センタ１０１の制御部２０１は、ＩＣカード１０４が不正かあるいは契約情報ＣＴ及び／又は署名Ｓ３が改竄されたと判断し通信部２０７からネットワーク１０２を介して端末１０３へエラー通知し（Ｓ４０９）、端末１０３の制御部３０１は通信部３０２からエラー通知を受信するとコンテンツ暗号鍵ダウンロード処理を中止する（Ｓ４２６）。

【０１６０】Ｓ４０８において、ＰＫｉｃ（Ｓ３）とＨ（ＣＴ）が一致した場合、管理センタ１０１の制御部２０１は、契約情報ＣＴの発行者がＩＣカード１０４である特定しかつ契約情報ＣＴ及び／又は署名Ｓ３に改竄が加えられていないと判断し、課金データベース２１２を契約情報ＣＴにより更新する（Ｓ４１０）。

【０１６１】次に管理センタ１０１の制御部２０１は、契約情報ＣＴに含まれるコンテンツのタイトルに対応したコンテンツ暗号鍵ＣＫをコンテンツ暗号鍵記憶部２０９から読み出し、コンテンツ暗号鍵ＣＫを圧縮部２０４

にてハッシュ関数を用いて圧縮しH（CK）を生成し、管理センタ秘密鍵記憶部２０８に記憶している管理センタ秘密鍵ＳＫｃｎｔを用いてH（CK）を暗号部２０３で暗号化することによりコンテンツ暗号鍵への管理センタ秘密鍵による署名Ｓ４を生成する（Ｓ４１１）。

【０１６２】次に上記の再生装置公開鍵の転送処理によって正常と確認された再生装置公開鍵ＰＫｐｌを用いて、暗号部２０３にてコンテンツ暗号鍵ＣＫと署名Ｓ４を暗号化しＰＫｐｌ（CK，Ｓ４）を生成する（Ｓ４１２）。

【０１６３】次に圧縮部２０４にてハッシュ関数を用いてＰＫｐｌ（CK，Ｓ４）と契約情報ＣＴを圧縮しH（ＰＫｐｌ（CK，Ｓ４），CT）を生成し、暗号部２０３にて管理センタ秘密鍵ＳＫｃｎｔを用いて、H（ＰＫｐｌ（CK，Ｓ４），CT）を暗号化し署名Ｓ５を生成する（Ｓ４１３）。

【０１６４】次に暗号部２０３にてＩＣカード公開鍵ＰＫｉｃを用いて、暗号化されたコンテンツ暗号鍵ＰＫｐｌ（CK，Ｓ４）と契約情報ＣＴと署名Ｓ５を暗号化しＰＫｉｃ（ＰＫｐｌ（CK，Ｓ４），CT，Ｓ５）を生成する（Ｓ４１４）。

【０１６５】次にコンテンツ暗号鍵ダウンロード要求に対するコンテンツ暗号鍵データとしてＰＫｉｃ（ＰＫｐｌ（CK，Ｓ４），CT，Ｓ５）を通信部２０７からネットワーク１０２を介して端末１０３へ送信する（Ｓ４１５）。

【０１６６】端末１０３の制御部３０１は通信部３０２からコンテンツ暗号鍵データＰＫｉｃ（ＰＫｐｌ（CK，Ｓ４），CT，Ｓ５）を受信すると、ＩＣカード入出力部３０３を介してＩＣカード１０４へコンテンツ暗号鍵データＰＫｉｃ（ＰＫｐｌ（CK，Ｓ４），CT，Ｓ５）と共にコンテンツ暗号鍵記憶要求を送信する（Ｓ４１６）。

【０１６７】ＩＣカード１０４の制御部４０１は入出力部４０２からコンテンツ暗号鍵記憶要求とコンテンツ暗号鍵データＰＫｉｃ（ＰＫｐｌ（CK，Ｓ４），CT，Ｓ５）を受信すると、復号部４０３にてＩＣカード秘密鍵記憶部４０８に記憶しているＩＣカード秘密鍵ＳＫｉｃを用いてＰＫｉｃ（ＰＫｐｌ（CK，Ｓ４），CT，Ｓ５）を復号しＰＫｐｌ（CK，Ｓ４）と契約情報ＣＴと署名Ｓ５を生成する（Ｓ４１７）。

【０１６８】次に復号部４０３にて管理センタ公開鍵記憶部４０９に記憶している管理センタ公開鍵ＰＫｃｎｔを用いて署名Ｓ５を復号しＰＫｃｎｔ（Ｓ５）を生成し、圧縮部４０５にてハッシュ関数を用いてＰＫｐｌ（CK，Ｓ４）と契約情報ＣＴを圧縮しH（ＰＫｐｌ（CK，Ｓ４），CT）を生成し、認証部４０７にてＰＫｃｎｔ（Ｓ５）とH（ＰＫｐｌ（CK，Ｓ４），CT）を照合する（Ｓ４１８）。

【０１６９】Ｓ４１９において、ＰＫｃｎｔ（Ｓ５）とH（ＰＫｐｌ（CK，Ｓ４），CT）が不一致である場合、ＩＣカード１０４の制御部４０１は、受信したデータは管理センタ１０１に成りすました装置からの不正なデータであるかあるいは改竄を加えられたデータであると判断し入出力部４０２を介して端末１０３へエラー通知を送信し（Ｓ４２０）、端末１０３の制御部３０１はＩＣカード入出力部３０３からエラー通知を受信するとコンテンツ暗号鍵ダウンロード処理を中止する（Ｓ４２６）。

【０１７０】Ｓ４１９において、ＰＫｃｎｔ（Ｓ５）とH（ＰＫｐｌ（CK，Ｓ４），CT）が一致した場合、ＩＣカード１０４の制御部４０１は、受信したデータの発行者は管理センタ１０１であると特定し、かつ受信したデータは改竄されていないと判断し、契約情報ＣＴ中の契約期限データＴをタイマ４１３へセットし（Ｓ４２１）、暗号化コンテンツ暗号鍵ＰＫｐｌ（CK，Ｓ４）をコンテンツ暗号鍵記憶部４１２へセットする（Ｓ４２２）。

【０１７１】次にＩＣカード１０４の制御部４０１は入出力部４０２を介して端末１０３へコンテンツ暗号鍵記憶要求に対しての正常応答を送信し（Ｓ４２３）、端末１０３の制御部３０１はＩＣカード入出力部３０３から正常終了を受信するとコンテンツ記憶部３０７からコンテンツデータをコンテンツ記憶媒体１０５へ書き込む（Ｓ４２４）。

【０１７２】コンテンツ記録媒体１０５へのコンテンツデータの書き込みが終了するとユーザはＩＣカード１０４とコンテンツ記録媒体１０５を持ち帰る（Ｓ４２５）。

【０１７３】図１０は図１の再生装置１０６とＩＣカード１０４とコンテンツ記憶媒体１０５を利用してコンテンツを再生する処理のタイムチャートを示している。

【０１７４】まずユーザは再生装置１０６へＩＣカード１０４を接続し、再生装置１０６とＩＣカード１０４は相互認証を行う（Ｓ５０１）。ＩＣカード１０４と再生装置１０３の相互認証は既に説明したので、ここでは省略する。

【０１７５】再生装置１０６の制御部５０１は操作入力部５０８からのコンテンツの再生指示（Ｓ５０２）により、ＩＣカード入出力部５０２を介してＩＣカード１０４へコンテンツ暗号鍵の送信を要求する（Ｓ５０３）。

【０１７６】ＩＣカード１０４の制御部４０１は入出力部４０２からコンテンツ暗号鍵の送信要求を受信すると（Ｓ５０４）、コンテンツ暗号鍵記憶部４１２にコンテンツ暗号鍵が存在しているか確認する（Ｓ５０５）。

【０１７７】Ｓ５０５において、コンテンツ暗号記憶部４１２にコンテンツ暗号鍵が無い場合、ＩＣカード１０４の制御部４０１は入出力部４０２を介して再生装置１０６へコンテンツ暗号鍵の消去通知を送信し（Ｓ５０６）、再生装置１０６の制御部５０１はコンテンツ暗号

鍵の消去通知を受信するとコンテンツ再生不可としてコンテンツ再生処理を終了する（Ｓ５２０）。

【０１７８】Ｓ５０５において、コンテンツ暗号記憶部４１２にコンテンツ暗号鍵がある場合、ＩＣカード１０４の制御部４０１は、コンテンツ暗号鍵記憶部４１２から暗号化されたコンテンツ暗号鍵ＰＫｐｌ（ＣＫ，Ｓ４）を、タイマ４１３からタイマ値ｔを読み出し（Ｓ５０８）、圧縮部４０５にてハッシュ関数を用いてコンテンツ暗号鍵ＰＫｐｌ（ＣＫ，Ｓ４）とタイマ値ｔを圧縮しＨ（ＰＫｐｌ（ＣＫ，Ｓ４），ｔ）を生成し、暗号部４０４にてＩＣカード秘密鍵記憶部４０８に記憶されているＩＣカード秘密鍵ＳＫｉｃを用いてＨ（ＰＫｐｌ（ＣＫ，Ｓ４），ｔ）を暗号化することにより署名Ｓ６を生成する（Ｓ５０９）。

【０１７９】次にＩＣカード１０４の制御部４０１は再生装置公開鍵により暗号化されているコンテンツ暗号鍵ＰＫｐｌ（ＣＫ，Ｓ４）とタイマ値ｔと署名Ｓ６を入出力部４０２を介して再生装置１０６へ送信する（Ｓ５１０）。

【０１８０】再生装置１０６の制御部５０１はＩＣカード入出力部５０２から再生装置公開鍵により暗号化されているコンテンツ暗号鍵ＰＫｐｌ（ＣＫ，Ｓ４）とタイマ値ｔと署名Ｓ６を受信すると、復号部５０３にて上記の相互認証で正常と確認されたＩＣカード公開鍵ＰＫｉｃを用いて署名Ｓ６を復号しＰＫｉｃ（Ｓ６）を生成し、圧縮部５０５にてハッシュ関数を用いてコンテンツ暗号鍵ＰＫｐｌ（ＣＫ，Ｓ４）とタイマ値ｔを圧縮しＨ（ＰＫｐｌ（ＣＫ，Ｓ４），ｔ）を生成し、認証部５０７にてＰＫｉｃ（Ｓ６）とＨ（ＰＫｐｌ（ＣＫ，Ｓ４），ｔ）を照合する（Ｓ５１１）。

【０１８１】Ｓ５１２において、ＰＫｉｃ（Ｓ６）とＨ（ＰＫｐｌ（ＣＫ，Ｓ４），ｔ）が不一致である場合、再生装置１０６の制御部５０１は、受信したデータは正当なＩＣカードになりすましたＩＣカードからのデータであるか又はＩＣカード１０４から受信したデータは改竄されていると判断し、再生不可として再生処理を終了する（Ｓ５２０）。

【０１８２】Ｓ５１２において、ＰＫｉｃ（Ｓ６）とＨ（ＰＫｐｌ（ＣＫ，Ｓ４），ｔ）が一致した場合、再生装置１０６の制御部５０１はタイマ値ｔをタイマ５１３へセット（Ｓ５１３）する。

【０１８３】次に再生装置１０６の制御部５０１は復号部５０３にて再生装置秘密鍵記憶部５１０に記憶されている再生装置秘密鍵ＳＫｐｌを用いて再生装置公開鍵により暗号化されているコンテンツ暗号鍵ＰＫｐｌ（ＣＫ，Ｓ４）を復号しＣＫと署名Ｓ４を生成する（Ｓ５１４）。

【０１８４】次に復号部５０３にて管理センタ公開鍵記憶部５１１に記憶されている管理センタ公開鍵ＰＫｃｎｔを用いて署名Ｓ４を復号しＰＫｃｎｔ（Ｓ４）を生成し、圧縮部５０５にてハッシュ関数を用いてＣＫを圧縮しＨ（ＣＫ）を生成し、認証部５０７でＰＫｃｎｔ（Ｓ４）とＨ（ＣＫ）を照合する（Ｓ５１５）。

【０１８５】Ｓ５１６において、ＰＫｃｎｔ（Ｓ４）とＨ（ＣＫ）が不一致である場合、再生装置１０６の制御部５０１は、受信したデータが管理センタ１０１が発行したデータではないかあるいはデータが改竄されていると判断し再生不可として再生処理を終了する（Ｓ５２０）。

【０１８６】Ｓ５１６において、ＰＫｃｎｔ（Ｓ４）とＨ（ＣＫ）が一致した場合、再生装置１０６の制御部５０１はコンテンツ暗号鍵ＣＫをコンテンツ暗号鍵記憶部５１４へセットする（Ｓ５１７）。

【０１８７】次に、再生装置１０６の制御部５０１はコンテンツ記録媒体入出力部５０９を介してコンテンツ記録媒体１０５からコンテンツデータを読み出し、コンテンツ再生部５１６にてコンテンツ暗号鍵記憶部５１５に記憶されているコンテンツ暗号鍵ＣＫを用いてコンテンツデータを復号し（Ｓ５１８）、コンテンツ再生を行う（Ｓ５１９）。

【０１８８】

【発明の効果】以上説明したように本発明によれば、以下の効果が奏される。

【０１８９】第１に、再生装置の公開鍵証明書をＩＣカードへ記憶することで再生をすることが可能な再生装置を安全に限定することかできる。

【０１９０】第２に、コンテンツをレンタルする前に再生装置の公開鍵証明書をＩＣカードへ記憶することで、再生装置の機種を安全かつ柔軟に変更することが可能であり、変更後の再生装置のみを再生をすることができる再生装置として安全に限定できる。

【０１９１】第３に、有効なコンテンツ暗号鍵、再生期限情報及び公開鍵証明書は管理センタが発行したものに限定されるので、有効なコンテンツ暗号鍵、再生期限情報及び公開鍵証明書は一元管理の基に保証され、従って、安全なコンテンツの流通が可能になる。

【０１９２】第４に、ＩＣカードの内部に再生期限情報を記憶しリアルタイムに再生期限を減ずる機能を有することで、再生期限の改竄を防止できる。

【０１９３】第５に、ＩＣカードならびに再生装置の内部に再生期限を過ぎるとコンテンツ再生に必要なコンテンツ暗号鍵を消去する機能を有することで、耐タンパ性を向上できる。

【図面の簡単な説明】

【図１】本発明の実施の形態におけるレンタルコンテンツ流通システムを示すブロック図である。

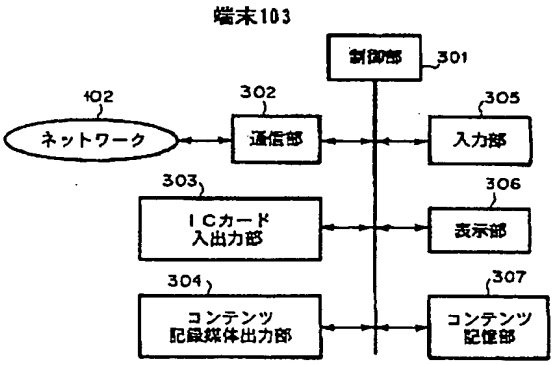
【図２】本発明の実施の形態における管理センタを示すブロック図である。

【図３】本発明の実施の形態における端末を示すブロック図である。

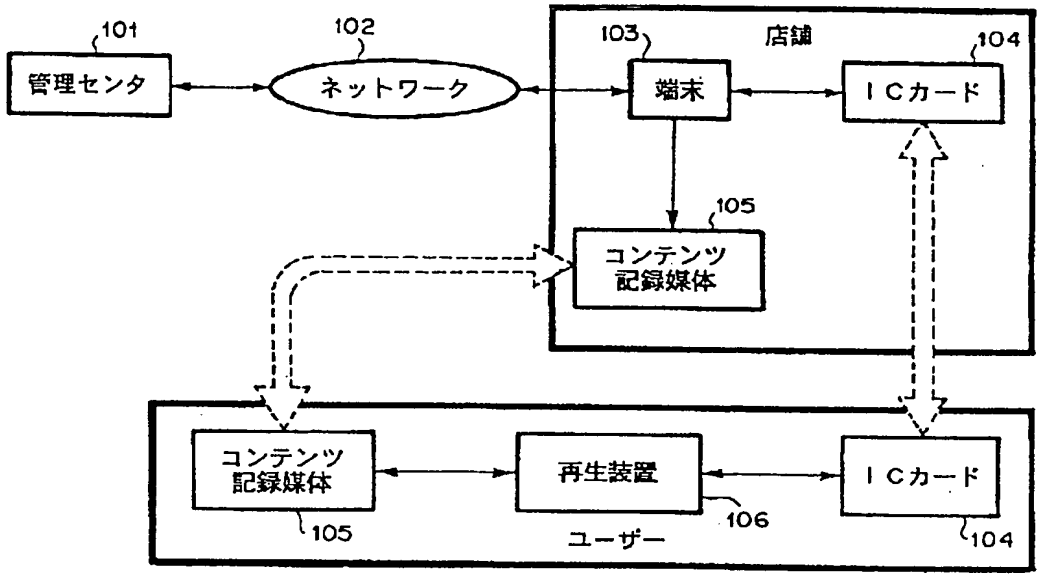
【図４】本発明の実施の形態におけるＩＣカードを示すブロック図である。
【図５】本発明の実施の形態における再生装置を示すブロック図である。
【図６】本発明の実施の形態におけるＩＣカードと再生装置の相互認証を示すタイムチャートである。
【図７】本発明の実施の形態におけるＩＣカードと管理センタの相互認証を示すタイムチャートである。
【図８】本発明の実施の形態におけるＩＣカードから管理センタへ再生装置公開鍵証明書の転送を示すタイムチャートである。
【図９】本発明の実施の形態における管理センタからＩＣカードへのコンテンツ暗号鍵のダウンロードを示すタイムチャートである。
【図１０】本発明の実施の形態におけるコンテンツ再生を示すタイムチャートである。
【符号の説明】

１０１	管理センタ
１０２	ネットワーク
１０３	端末
１０４	ＩＣカード
１０５	コンテンツ記録媒体
１０６	再生装置
２０１	制御部
２０２	復号部
２０３	暗号部
２０４	圧縮部
２０５	乱数発生部
２０６	認証部
２０７	通信部
２０８	管理センタ秘密鍵記憶部
２０９	管理センタ公開鍵記憶部
２１０	コンテンツ暗号鍵記憶部
２１１	公開鍵データベース
２１２	課金情報データベース
３０１	制御部
３０２	通信部
３０３	ＩＣカード入出力部
３０４	コンテンツ記録媒体入出力部
３０５	入力部
３０６	表示部
３０７	コンテンツ記憶部
４０１	制御部
４０２	入出力部
４０３	復号部
４０４	暗号部
４０５	圧縮部
４０６	乱数発生部
４０７	認証部
４０８	ＩＣカード秘密鍵記憶部
４０９	管理センタ公開鍵記憶部
４１０	ＩＣカード公開鍵証明書記憶部
４１１	再生装置公開鍵証明書記憶部
４１２	コンテンツ暗号鍵記憶部
４１３	タイマ
４１４	電池
５０１	制御部
５０２	ＩＣカード入出力部
５０３	復号部
５０４	暗号部
５０５	圧縮部
５０６	乱数発生部
５０７	認証部
５０８	操作入力部
５０９	コンテンツ記録媒体入出力部
５１０	再生装置秘密鍵記憶部
５１１	管理センタ公開鍵記憶部
５１２	再生装置公開鍵証明書
５１３	タイマ
５１４	コンテンツ暗号鍵記憶部
５１５	コンテンツ暗号鍵復号部
５１６	コンテンツ再生部

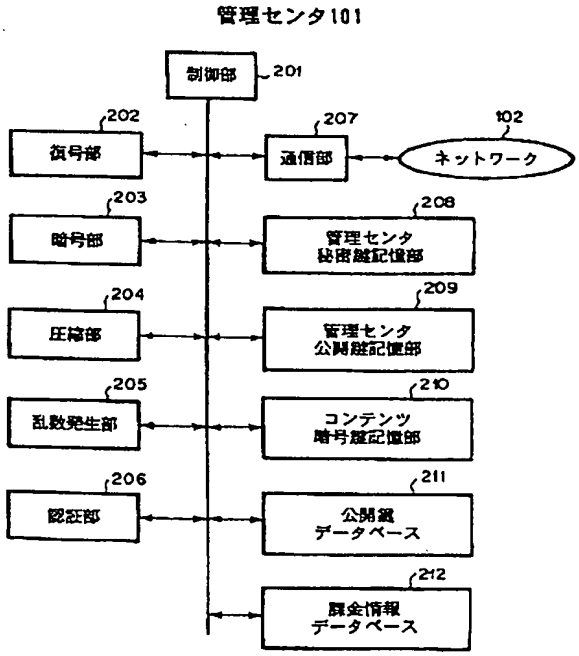
【図３】



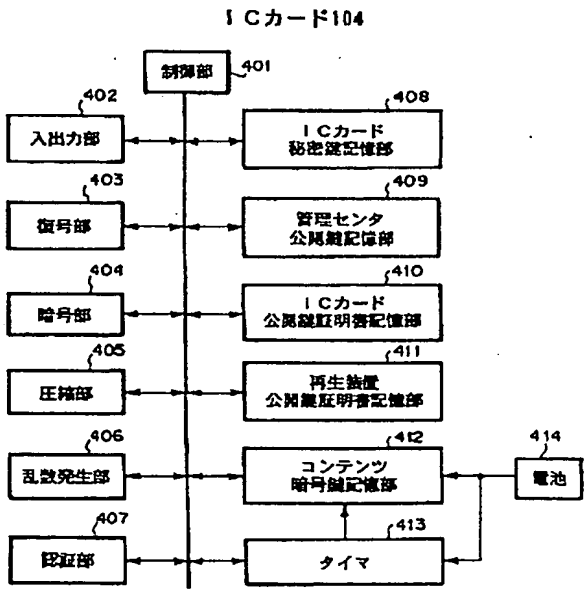
【図１】


101
管理センタ
102
ネットワーク
103
店舗
端末
104
ＩＣカード
105
コンテンツ
記録媒体
コンテンツ
記録媒体
105
再生装置
106
ＩＣカード
104
ユーザー

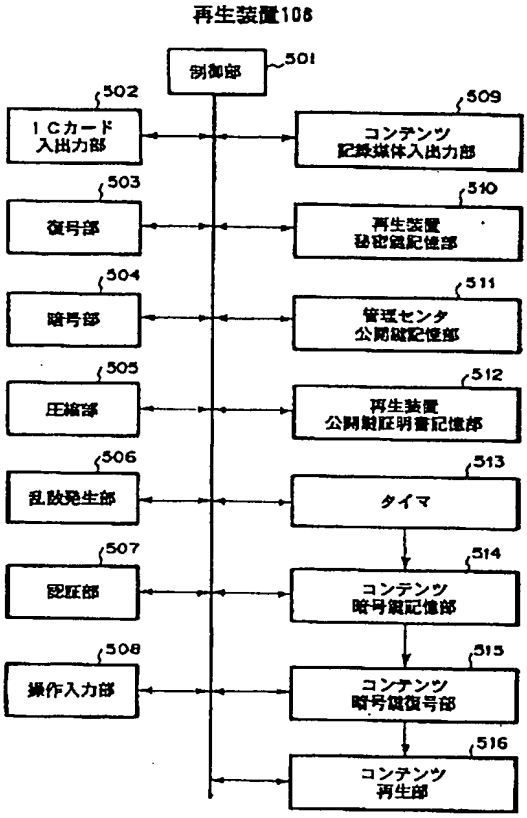
【図２】


管理センタ101
制御部
201
202
復号部
207
通信部
102
ネットワーク
203
暗号部
208
管理センタ
秘密鍵記憶部
204
圧縮部
209
管理センタ
公開鍵記憶部
205
乱数発生部
210
コンテンツ
暗号鍵記憶部
206
認証部
211
公開鍵
データベース
212
課金情報
データベース

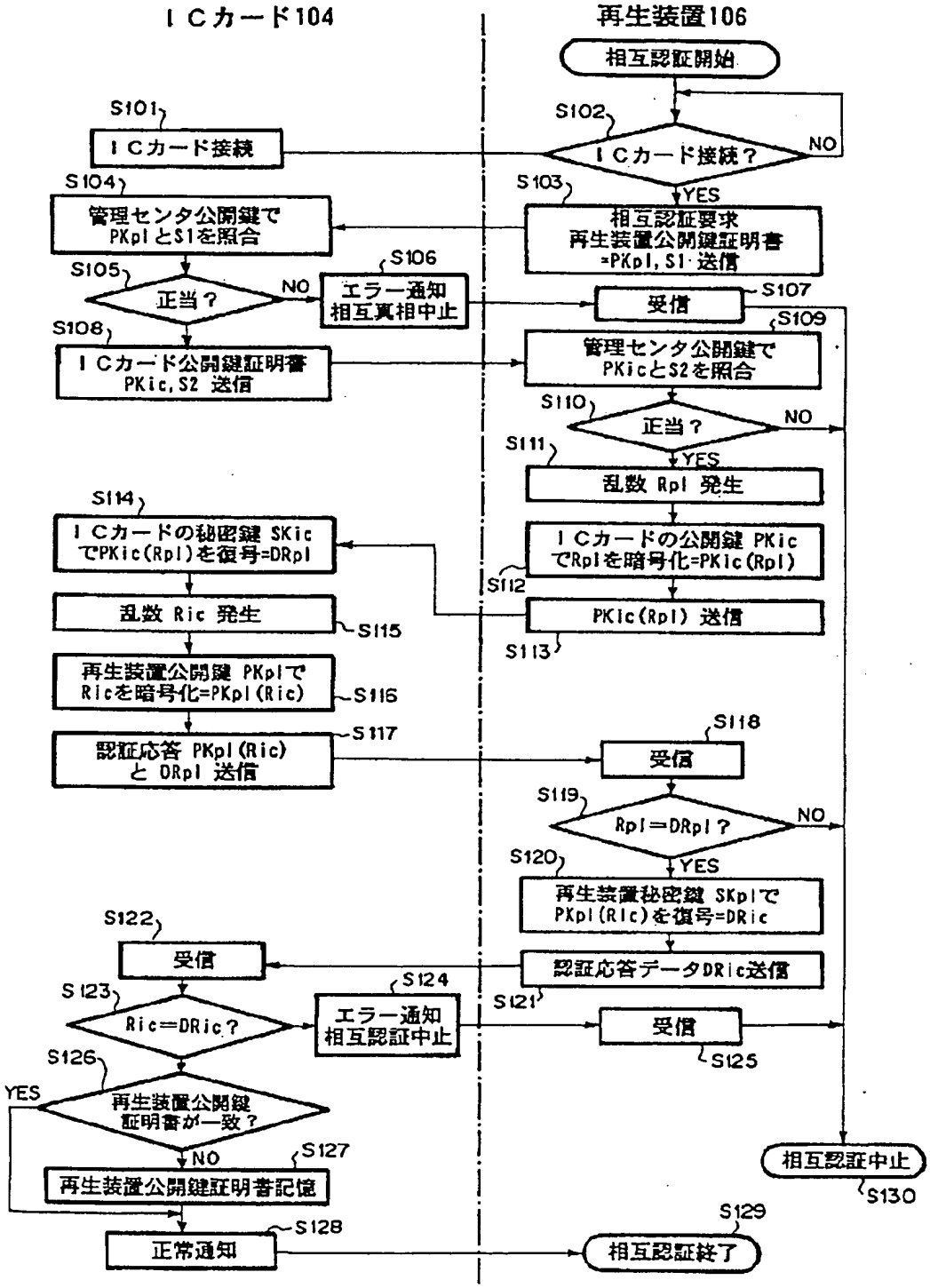
【図４】


ＩＣカード104
制御部
401
402
入出力部
408
ＩＣカード
秘密鍵記憶部
403
復号部
409
管理センタ
公開鍵記憶部
404
暗号部
410
ＩＣカード
公開鍵証明書記憶部
405
圧縮部
411
再生装置
公開鍵証明書記憶部
406
乱数発生部
412
コンテンツ
暗号鍵記憶部
414
電池
407
認証部
413
タイマ

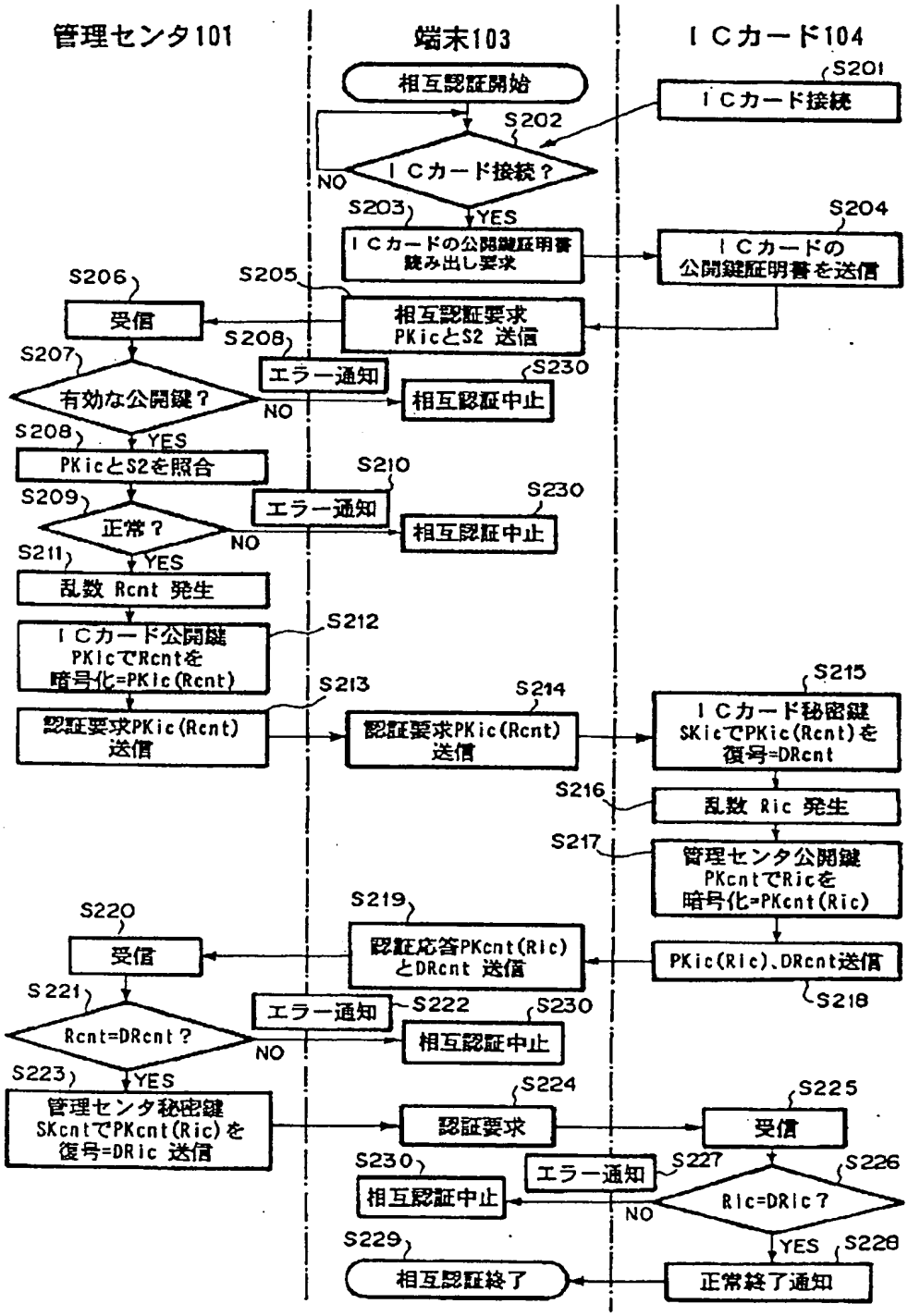
【図５】


再生装置108
制御部
501
502
ＩＣカード
入出力部
503
復号部
504
暗号部
505
圧縮部
506
乱数発生部
507
認証部
508
操作入力部
509
コンテンツ
記録媒体入出力部
510
再生装置
秘密鍵記憶部
511
管理センタ
公開鍵記憶部
512
再生装置
公開鍵証明書記憶部
513
タイマ
514
コンテンツ
暗号鍵記憶部
515
コンテンツ
暗号鍵復号部
516
コンテンツ
再生部

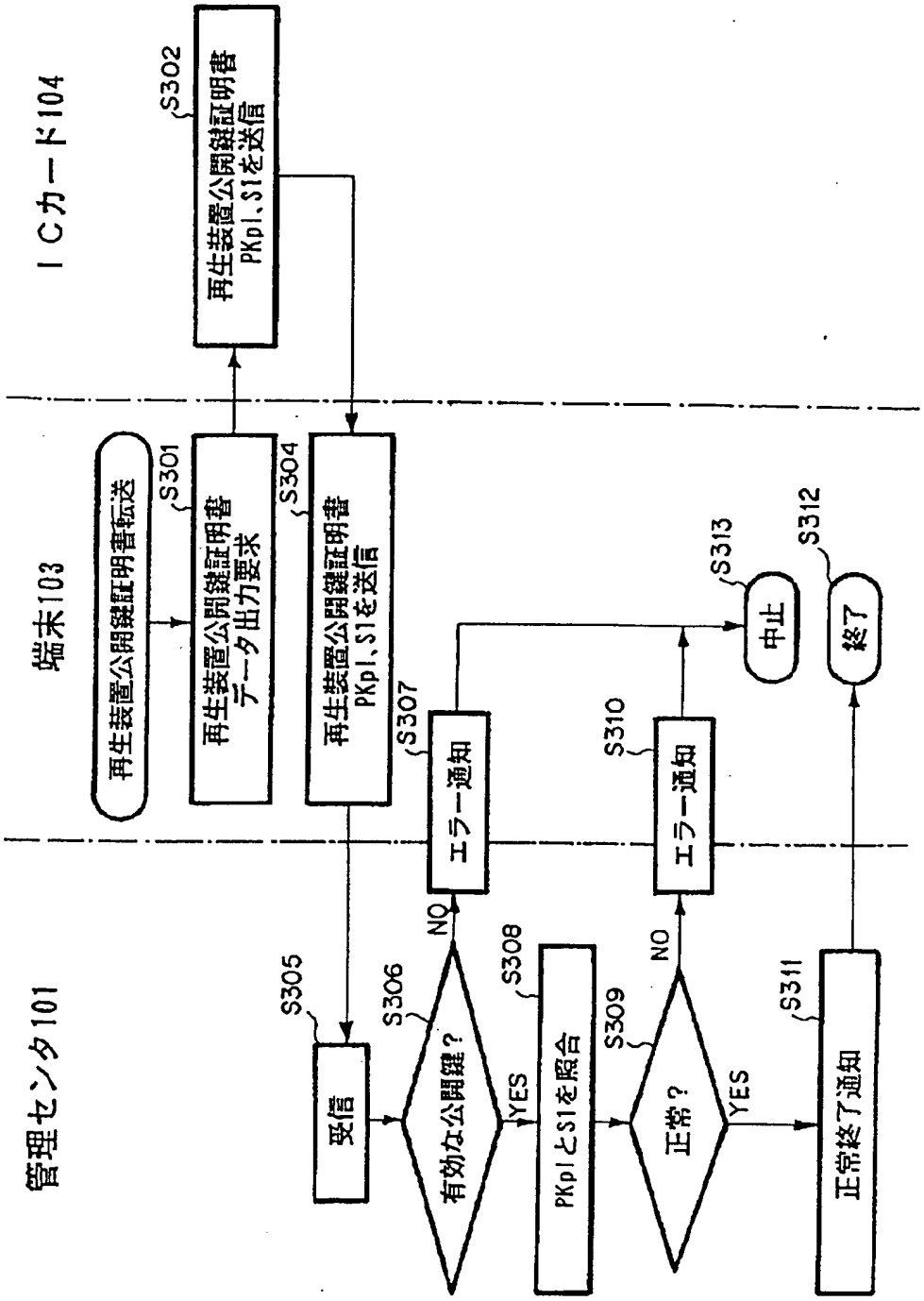
【図６】


ＩＣカード104
再生装置106
相互認証開始
S101
ＩＣカード接続
S102
ＩＣカード接続？
NO
YES
S103
相互認証要求
再生装置公開鍵証明書
=PKpl, S1 送信
S104
管理センタ公開鍵で
PKplとS1を照合
S105
正当？
NO
S106
エラー通知
相互真相中止
S107
受信
S108
ＩＣカード公開鍵証明書
PKic, S2 送信
S109
管理センタ公開鍵で
PKicとS2を照合
S110
正当？
NO
YES
S111
乱数 Rpl 発生
S112
ＩＣカードの公開鍵 PKic
でRplを暗号化=PKic(Rpl)
S113
PKic(Rpl) 送信
S114
ＩＣカードの秘密鍵 SKic
でPKic(Rpl)を復号=DRpl
S115
乱数 Ric 発生
S116
再生装置公開鍵 PKplで
Ricを暗号化=PKpl(Ric)
S117
認証応答 PKpl(Ric)
と DRpl 送信
S118
受信
S119
Rpl=DRpl？
NO
YES
S120
再生装置秘密鍵 SKplで
PKpl(Ric)を復号=DRic
S121
認証応答データDRic送信
S122
受信
S123
Ric=DRic？
S124
エラー通知
相互認証中止
S125
受信
S126
再生装置公開鍵
証明書が一致？
YES
NO
S127
再生装置公開鍵証明書記憶
S128
正常通知
S129
相互認証終了
相互認証中止
S130

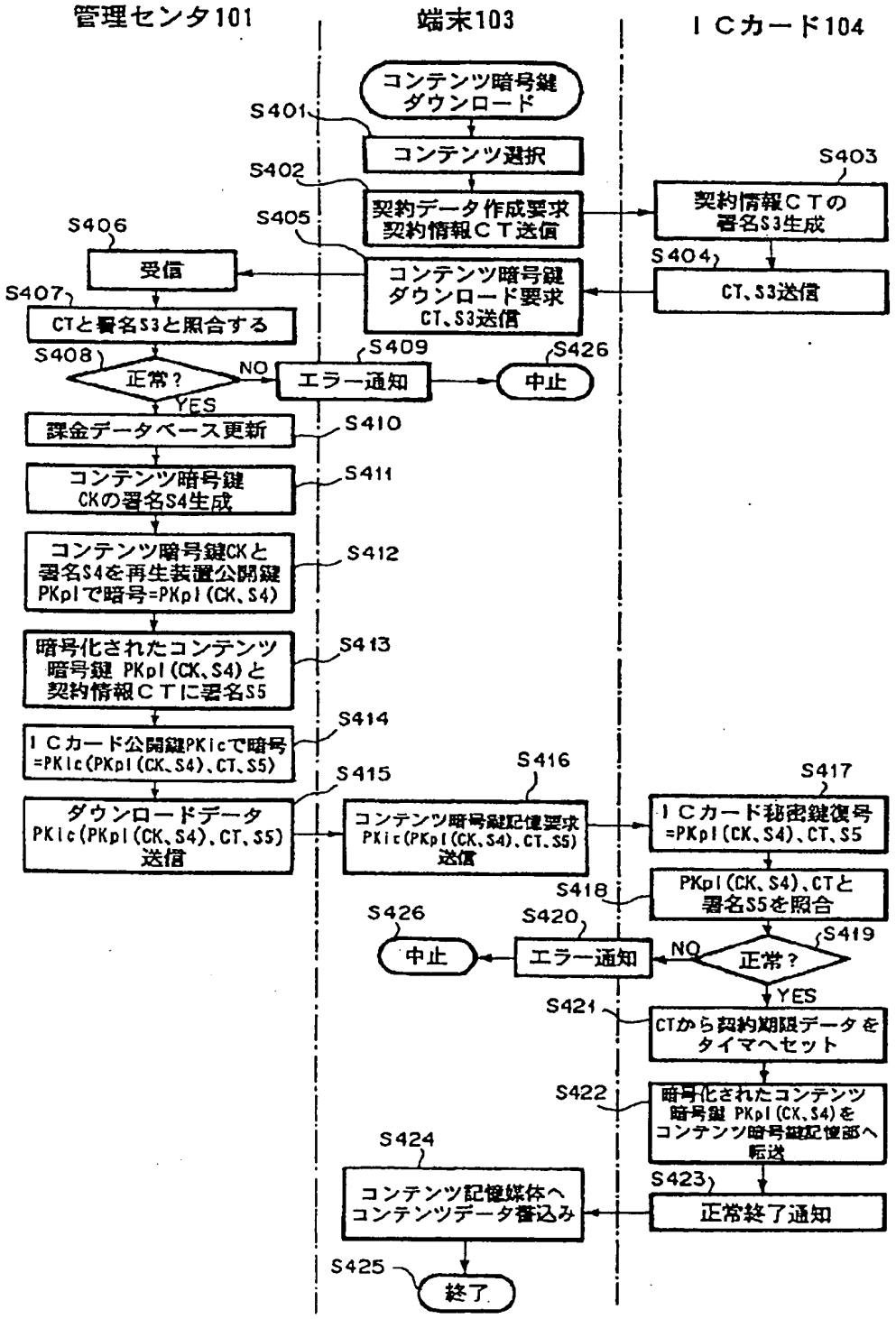
【図７】


管理センタ101
端末103
ＩＣカード104
相互認証開始
S201
ＩＣカード接続
S202
ＩＣカード接続？
NO
YES
S203
ＩＣカードの公開鍵証明書読み出し要求
S204
ＩＣカードの公開鍵証明書を送信
S205
相互認証要求 PKicとS2 送信
S206
受信
S207
有効な公開鍵？
NO
S208
エラー通知
S230
相互認証中止
YES
S208
PKicとS2を照合
S209
正常？
NO
S210
エラー通知
S230
相互認証中止
YES
S211
乱数 Rcnt 発生
S212
ＩＣカード公開鍵 PKicでRcntを暗号化=PKic(Rcnt)
S213
認証要求PKic(Rcnt) 送信
S214
認証要求PKic(Rcnt) 送信
S215
ＩＣカード秘密鍵 SKicでPKic(Rcnt)を復号=DRcnt
S216
乱数 Ric 発生
S217
管理センタ公開鍵 PKcntでRicを暗号化=PKcnt(Ric)
S218
PKic(Ric)、DRcnt送信
S219
認証応答PKcnt(Ric) とDRcnt 送信
S220
受信
S221
Rcnt=DRcnt？
NO
S222
エラー通知
S230
相互認証中止
YES
S223
管理センタ秘密鍵 SKcntでPKcnt(Ric)を復号=DRic 送信
S224
認証要求
S225
受信
S227
エラー通知
S230
相互認証中止
S226
Ric=DRic？
NO
YES
S228
正常終了通知
S229
相互認証終了

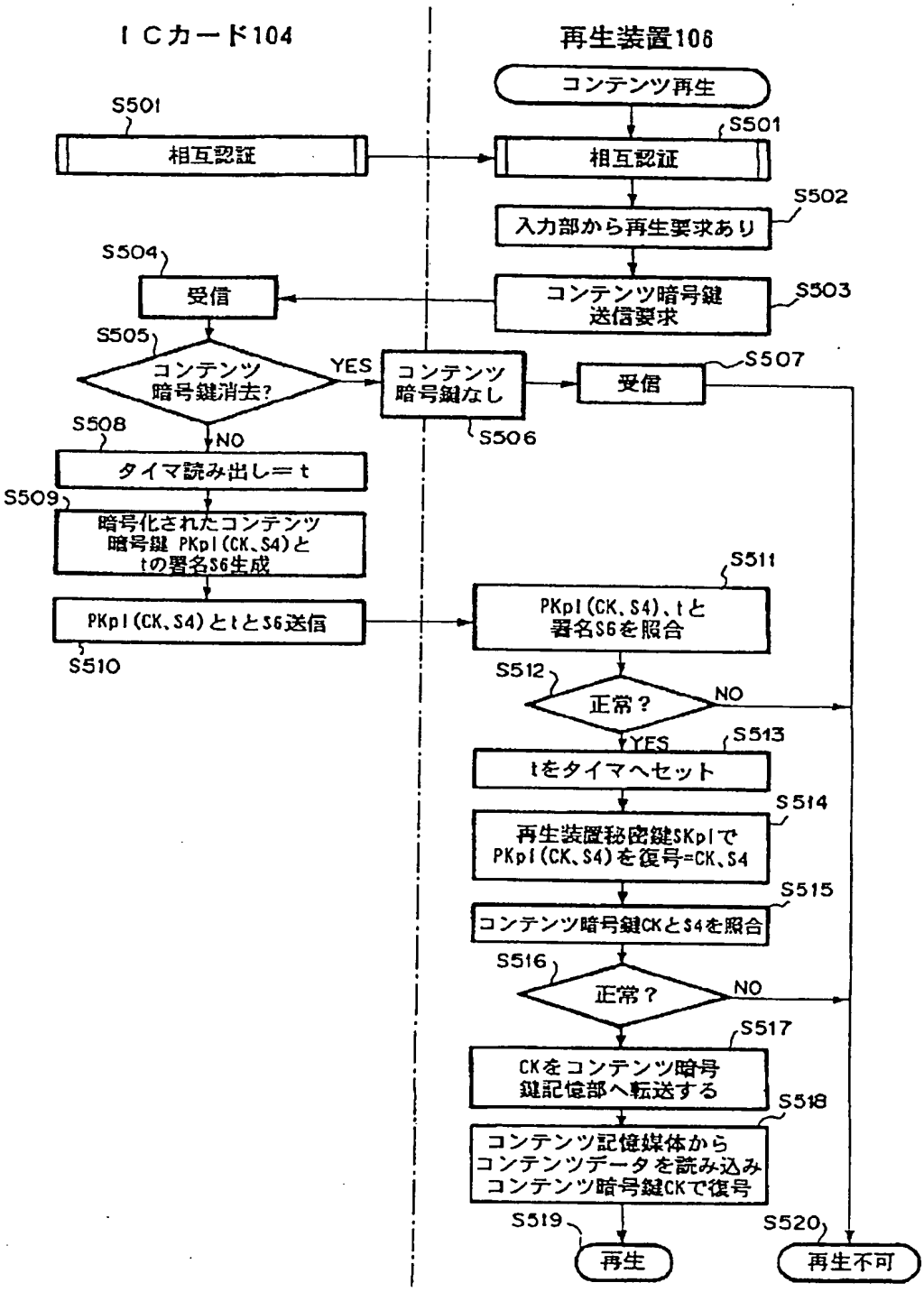
【図８】


ＩＣカード104
端末103
管理センタ101
再生装置公開鍵証明書転送
S301
再生装置公開鍵証明書
データ出力要求
S302
再生装置公開鍵証明書
PKp1、S1を送信
S304
再生装置公開鍵証明書
PKp1、S1を送信
S305
受信
S306
有効な公開鍵？
NO
YES
S307
エラー通知
S308
PKp1とS1を照合
S309
正常？
NO
YES
S310
エラー通知
S311
正常終了通知
S312
終了
S313
中止

【図９】


管理センタ101
端末103
ＩＣカード104
コンテンツ暗号鍵ダウンロード
S401
コンテンツ選択
S402
契約データ作成要求 契約情報ＣＴ送信
S403
契約情報ＣＴの署名S3生成
S404
CT、S3送信
S405
コンテンツ暗号鍵ダウンロード要求 CT、S3送信
S406
受信
S407
CTと署名S3と照合する
S408
正常？
NO
S409
エラー通知
S426
中止
YES
課金データベース更新
S410
コンテンツ暗号鍵CKの署名S4生成
S411
コンテンツ暗号鍵CKと署名S4を再生装置公開鍵PKplで暗号=PKpl(CK、S4)
S412
暗号化されたコンテンツ暗号鍵 PKpl(CK、S4)と契約情報ＣＴに署名S5
S413
ＩＣカード公開鍵PKicで暗号=PKic(PKpl(CK、S4)、CT、S5)
S414
ダウンロードデータ PKic(PKpl(CK、S4)、CT、S5)送信
S415
コンテンツ暗号鍵記憶要求 PKic(PKpl(CK、S4)、CT、S5)送信
S416
ＩＣカード秘密鍵復号=PKpl(CK、S4)、CT、S5
S417
PKpl(CK、S4)、CTと署名S5を照合
S418
正常？
S419
NO
エラー通知
S420
中止
S426
YES
CTから契約期限データをタイマへセット
S421
暗号化されたコンテンツ暗号鍵 PKpl(CK、S4)をコンテンツ暗号鍵記憶部へ転送
S422
正常終了通知
S423
コンテンツ記憶媒体へコンテンツデータ書込み
S424
終了
S425

【図１０】


ＩＣカード104
再生装置106
コンテンツ再生
S501
相互認証
S501
相互認証
S502
入力部から再生要求あり
S504
受信
コンテンツ暗号鍵
送信要求
S503
S505
コンテンツ
暗号鍵消去?
YES
コンテンツ
暗号鍵なし
S507
受信
S506
S508
NO
タイマ読み出し＝ｔ
S509
暗号化されたコンテンツ
暗号鍵 PKpl(CK、S4)と
tの署名S6生成
PKpl(CK、S4)とtとS6送信
S510
S511
PKpl(CK、S4)、tと
署名S6を照合
S512
正常？
NO
YES
S513
tをタイマへセット
S514
再生装置秘密鍵SKplで
PKpl(CK、S4)を復号=CK、S4
S515
コンテンツ暗号鍵CKとS4を照合
S516
正常？
NO
S517
CKをコンテンツ暗号
鍵記憶部へ転送する
S518
コンテンツ記憶媒体から
コンテンツデータを読み込み
コンテンツ暗号鍵CKで復号
S519
再生
S520
再生不可

フロントページの続き

(51)Int.Cl.⁷		識別記号
G06F	15/00	330
	17/60	ZEC
		140
		302
		342
		510
G06K	17/00	
	19/00	
	19/10	
H04L	9/32	

FI		テーマコード(参考)
G06F	15/00	330Z　5B085
	17/60	ZEC　5J104
		140
		302E
		342
		510
G06K	17/00	L
		T
	19/00	Q
		R
H04L	9/00	675B
		675D

(72)発明者　塚本　雄二
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　菊地　芳秀
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　舩矢　幸一
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　大塚　修
東京都港区芝五丁目７番１号　日本電気株式会社内

Fターム(参考)　5B017 AA03 BA05 BA07 BB10 CA16
5B035 AA15 BB09 BC00 CA29
5B049 AA05 BB00 BB58 CC08 CC21
DD01 DD04 EE01 EE23 EE28
FF03 FF04 GG04 GG07 GG10
5B058 CA27 KA02 KA04 KA13 KA33
KA35 YA20
5B082 EA12 GA02 GA12
5B085 AA08 AC12 AE12 AE13 AE29
BE07 BG03
5J104 AA07 AA09 AA12 AA16 EA06
JA21 KA02 KA05 LA03 LA06
MA02 NA02 NA35 NA37 NA38
NA40 NA42 PA10 PA14